PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-319932

(43)Date of publication of application : 31.10.2002

---

(51)Int.Cl. H04L 9/08
G11B 20/10

---

(21)Application number : 2001-120494 (71)Applicant : SONY CORP

(22)Date of filing : 19.04.2001 (72)Inventor : OKANOE TAKUMI

---

(54) DEVICE AND METHOD FOR RECORDING INFORMATION, DEVICE AND METHOD FOR REPRODUCING INFORMATION, AND PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a configuration capable of limiting a data processor to utilize contents.

SOLUTION: As a reproduction execution condition of contents stored on a removable storage device such as memory card, the device can acquire a contents key, which can be decoded by effective key block(EKB) processing. Further, the device performs recording processing to the removable storage device or the device designated in the case of contents purchasing processing can be set. Thus, even when a plurality of devices capable of decoding the same EKB exist, a device capable of reproducing the contents stored on the removable storage device can be limited to only one device.

LEGAL STATUS [Date of request for examination] 12.02.2003
[Date of sending the examiner's decision of rejection] 19.01.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] The storage means which stored the device node key (DNK) which becomes each node which constitutes the hierarchy tree structure which used as the leaf the information recording device with which plurality differs in the information recording device which records information on a record medium from the node key of a proper, and the leaf key of each information recording device proper, It has a cipher-processing means to perform cipher processing of the storing data to said record medium. Said cipher-processing means Cipher processing which applied the cryptographic key (Kcon) to the characteristic value of the specific data regenerative apparatus which reproduces the storing data of said record medium is performed. Generate the cryptographic key (Kst) applied to said storing data, and the storing data encryption processing by this cryptographic key (Kst) generates encryption data:Enc (Kst, DATA). The cryptographic key (Kcon) applied to cipher processing of said characteristic value The cryptographic

key data enciphered using the hierarchy tree configuration key stored in the validation key block (EKB) which enciphered the high order key of said hierarchy tree by a low order hierarchy's node key or the key of a leaf key which contains either at least are generated. Said encryption data, The information recording device characterized by having the configuration which performs processing which stores the data file containing said cryptographic key data, and said validation key block (EKB) in said record medium.

[Claim 2] It is the information recording device according to claim 1 which said specific data regenerative apparatus is said information recording device itself, and is characterized by said characteristic value being the characteristic value matched with said information recording device.

[Claim 3] Said information recording apparatus is a contents distribution terminal which performs distribution of contents. Said specific data regenerative apparatus It is a data regenerative apparatus using the download contents from said contents distribution terminal. Said characteristic value It is the information recording apparatus according to claim 1 characterized by being the configuration of performing cipher processing which is the characteristic value matched with said data regenerative apparatus, and applied said cryptographic key (Kcon) to the characteristic value matched with said data regenerative apparatus into which said information recording apparatus was inputted from the outside.

[Claim 4] The characteristic value of said data regenerative apparatus is an information recording device according to claim 1 characterized [at this data regenerative apparatus] by being discernment data of a proper the telephone number or the data regenerative apparatus of a proper.

[Claim 5] Said record medium is an information recording apparatus according to claim 1 characterized by being a removable removable record medium to said information recording apparatus.

[Claim 6] The hierarchy tree configuration key stored in said validation key block (EKB) is an information recording device according to claim 1 characterized by being root key:Kroot set up to the root which is the top-most-vertices node of this hierarchy tree.

[Claim 7] The hierarchy tree configuration key stored in said validation key block (EKB) is an information recording device according to claim 1 characterized by being a key acquirable [with decode processing of said validation key block (EKB) by said device node key (DNK)].

[Claim 8] The hierarchy tree configuration key stored in said validation key block (EKB) It is constituted as a key which can be updated. Said information recording device The

updated hierarchy tree configuration key which was stored in the validation key block (EKB) which enciphered the high order key of said hierarchy tree by a low order hierarchy's node key, or the key of a leaf key which contains either at least The information recording device according to claim 1 characterized by having the configuration acquired by decode processing of said validation key block (EKB) by said device node key (DNK).

[Claim 9] Said cipher-processing means is an information recording device according to claim 1 characterized by being the configuration which generates the cryptographic key (Kcon) to the characteristic value of said information recording device based on a random number.

[Claim 10] In the information regenerative apparatus which performs regeneration of the storing data stored in the record medium The storage means which stored the device node key (DNK) which becomes each node which constitutes the hierarchy tree structure which used as the leaf the information regenerative apparatus with which plurality differs from the node key of a proper, and a leaf key peculiar to each information ******, It has a cipher-processing means to perform decode processing of the storing data of said record medium. Said cipher-processing means The validation key block (EKB) which enciphered the high order key of said hierarchy tree stored in said record medium by a low order hierarchy's node key or the key of a leaf key which contains either at least is decoded using said device node key (DNK). The hierarchy tree configuration key stored in this validation key block (EKB) is acquired. Acquire a cryptographic key (Kcon) by decode processing of the cryptographic key data enciphered using said hierarchy tree configuration key stored in said record medium, and characteristic value of an information regenerative apparatus own [said] is received. Storing encryption data perform cipher processing which applied said cryptographic key (Kcon), generate the decode key (Kst) applied to said storing data, and according to this decode key (Kst): The information regenerative apparatus characterized by having the configuration which performs decode processing of Enc (Kst, DATA).

[Claim 11] The characteristic value of said information regenerative apparatus is an information regenerative apparatus according to claim 10 characterized [at this information regenerative apparatus] by being discernment data of a proper the telephone number or the information regenerative apparatus of a proper.

[Claim 12] Said record medium is an information regenerative apparatus according to claim 10 characterized by being a removable removable record medium to said information regenerative apparatus.

[Claim 13] The hierarchy tree configuration key stored in said validation key block

(EKB) is an information regenerative apparatus according to claim 10 characterized by being root key:Kroot set up to the root which is the top-most-vertices node of this hierarchy tree.

[Claim 14] The hierarchy tree configuration key stored in said validation key block (EKB) It is constituted as a key which can be updated. Said information regenerative apparatus The updated hierarchy tree configuration key which was stored in the validation key block (EKB) which enciphered the high order key of said hierarchy tree by a low order hierarchy's node key, or the key of a leaf key which contains either at least The information regenerative apparatus according to claim 10 characterized by having the configuration acquired by decode processing of said validation key block (EKB) by said device node key (DNK).

[Claim 15] The storage means which stored the device node key (DNK) which becomes each node which constitutes the hierarchy tree structure which used as the leaf the information recording device with which plurality differs from the node key of a proper, and the leaf key of each information recording device proper, In the information record approach for said record medium in the information recording device which has a cipher-processing means to perform cipher processing of the storing data to a record medium Cipher processing which applied the cryptographic key (Kcon) to the characteristic value of the specific data regenerative apparatus which reproduces the storing data of said record medium is performed. The step which generates the cryptographic key (Kst) applied to said storing data, the storing data encryption processing by said cryptographic key (Kst) -- encryption data: -- with the step which generates Enc (Kst, DATA) The cryptographic key (Kcon) applied to cipher processing of said characteristic value The step which generates the cryptographic key data enciphered using the hierarchy tree configuration key stored in the validation key block (EKB) which enciphered the high order key of said hierarchy tree by a low order hierarchy's node key, or the key of a leaf key which contains either at least, and said encryption data, The information record approach characterized by having the step which stores the data file containing said cryptographic key data, and said validation key block (EKB) in said record medium.

[Claim 16] It is the information record approach according to claim 15 which said specific data regenerative apparatus is said information recording device itself, and is characterized by said characteristic value being the characteristic value matched with said information recording device.

[Claim 17] Said information recording apparatus is a contents distribution terminal which performs distribution of contents. Said specific data regenerative apparatus It is

a data regenerative apparatus using the download contents from said contents distribution terminal. Said characteristic value Are the characteristic value matched with said data regenerative apparatus, and the step which generates said cryptographic key (Kst) The information record approach according to claim 15 characterized by including the step which performs cipher processing which applied said cryptographic key (Kcon) from the outside to the characteristic value matched with said inputted data regenerative apparatus.

[Claim 18] The characteristic value of said data regenerative apparatus is the information record approach according to claim 15 characterized [at this data regenerative apparatus] by being discernment data of a proper the telephone number or the data regenerative apparatus of a proper.

[Claim 19] Said record medium is the information record approach according to claim 15 characterized by being a removable removable record medium to said information recording apparatus.

[Claim 20] The hierarchy tree configuration key stored in said validation key block (EKB) is the information record approach according to claim 15 characterized by being root key:Kroot set up to the root which is the top-most-vertices node of this hierarchy tree.

[Claim 21] The hierarchy tree configuration key stored in said validation key block (EKB) is the information record approach according to claim 15 characterized by being a key acquirable [with decode processing of said validation key block (EKB) by said device node key (DNK)].

[Claim 22] The hierarchy tree configuration key stored in said validation key block (EKB) It is constituted as a key which can be updated. Said information record approach Furthermore, the updated hierarchy tree configuration key which was stored in the validation key block (EKB) which enciphered the high order key of said hierarchy tree by a low order hierarchy's node key, or the key of a leaf key which contains either at least The information record approach according to claim 15 characterized by including the step which performs processing acquired by decode processing of said validation key block (EKB) by said device node key (DNK).

[Claim 23] Said information record approach is the information record approach according to claim 15 characterized by having further the step which generates the cryptographic key (Kcon) to the characteristic value of said information recording device based on a random number.

[Claim 24] The storage means which stored the device node key (DNK) which becomes each node which constitutes the hierarchy tree structure which used as the leaf the

information regenerative apparatus with which plurality differs from the node key of a proper, and a leaf key peculiar to each information ******, In the information playback approach of performing regeneration of the storing data stored in said record medium in the information regenerative apparatus which has a cipher-processing means to perform decode processing of the storing data of a record medium The validation key block (EKB) which enciphered the high order key of said hierarchy tree stored in said record medium by a low order hierarchy's node key or the key of a leaf key which contains either at least is decoded using said device node key (DNK). The step which acquires the hierarchy tree configuration key stored in this validation key block (EKB), The step which acquires a cryptographic key (Kcon) by decode processing of the cryptographic key data enciphered using said hierarchy tree configuration key stored in said record medium, Cipher processing which applied said cryptographic key (Kcon) is performed to characteristic value of an information regenerative apparatus own [said]. Storing encryption data generate the decode key (Kst) applied to said storing data, and according to this decode key (Kst): The information playback approach characterized by having the step which performs decode processing of Enc (Kst, DATA).

[Claim 25] The characteristic value of said information regenerative apparatus is the information playback approach according to claim 24 characterized [at this information regenerative apparatus] by being discernment data of a proper the telephone number or the information regenerative apparatus of a proper.

[Claim 26] Said record medium is the information playback approach according to claim 24 characterized by being a removable removable record medium to said information regenerative apparatus.

[Claim 27] The hierarchy tree configuration key stored in said validation key block (EKB) is the information playback approach according to claim 24 characterized by being root key:Kroot set up to the root which is the top-most-vertices node of this hierarchy tree.

[Claim 28] The hierarchy tree configuration key stored in said validation key block (EKB) It is constituted as a key which can be updated. Said information playback approach Furthermore, the updated hierarchy tree configuration key which was stored in the validation key block (EKB) which enciphered the high order key of said hierarchy tree by a low order hierarchy's node key, or the key of a leaf key which contains either at least The information playback approach according to claim 24 characterized by including the step acquired by decode processing of said validation key block (EKB) by said device node key (DNK).

[Claim 29] The storage means which stored the device node key (DNK) which becomes

each node which constitutes the hierarchy tree structure which used as the leaf the information recording device with which plurality differs from the node key of a proper, and the leaf key of each information recording device proper, It is the program which makes the information record processing to said record medium in the information recording device which has a cipher-processing means to perform cipher processing of the storing data to a record medium perform on computer system. Said program performs cipher processing which applied the cryptographic key (Kcon) to the characteristic value of the specific data regenerative apparatus which reproduces the storing data of said record medium. The step which generates the cryptographic key (Kst) applied to said storing data, the storing data encryption processing by said cryptographic key (Kst) -- encryption data: -- with the step which generates Enc (Kst, DATA) The cryptographic key (Kcon) applied to cipher processing of said characteristic value The step which generates the cryptographic key data enciphered using the hierarchy tree configuration key stored in the validation key block (EKB) which enciphered the high order key of said hierarchy tree by a low order hierarchy's node key, or the key of a leaf key which contains either at least, and said encryption data, The program characterized by having the step which stores the data file containing said cryptographic key data, and said validation key block (EKB) in said record medium.

[Claim 30] The storage means which stored the device node key (DNK) which becomes each node which constitutes the hierarchy tree structure which used as the leaf the information regenerative apparatus with which plurality differs from the node key of a proper, and a leaf key peculiar to each information ******, It can set to the information regenerative apparatus which has a cipher-processing means to perform decode processing of the storing data of a record medium. It is the program which makes regeneration of the storing data stored in said record medium perform on computer system. Said program The validation key block (EKB) which enciphered the high order key of said hierarchy tree stored in said record medium by a low order hierarchy's node key or the key of a leaf key which contains either at least is decoded using said device node key (DNK). The step which acquires the hierarchy tree configuration key stored in this validation key block (EKB), The step which acquires a cryptographic key (Kcon) by decode processing of the cryptographic key data enciphered using said hierarchy tree configuration key stored in said record medium, Cipher processing which applied said cryptographic key (Kcon) is performed to characteristic value of an information regenerative apparatus own [said]. Storing encryption data generate the decode key (Kst) applied to said storing data, and according to this decode key (Kst): The program characterized by having the step which performs decode processing of Enc (Kst, DATA).

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to a program at an information recording device, an information regenerative apparatus and the information record approach, the information playback approach, and a list. Especially, only in a just contents utilization device, activation of playback of various contents, such as music, an image, a game, and a program, is enabled, and it is related with a program at the information recording device which realized the configuration which eliminates migration playback of the inaccurate contents through a removable storage device, an information regenerative apparatus and the information record approach, the information playback approach, and a list.

[0002]

[Description of the Prior Art] The contents negotiation which circulates various software data (these are hereafter called contents (Content)), such as music data, a game program, and image data, through the storage of networks, such as the Internet, or a memory card, DVD, CD, etc., etc. which can be circulated prospers these days. PC (Personal Computer) with which a user owns these negotiation contents, a cellular phone, a data regenerative apparatus, or a game device receives immediate data, it stores in an internal memory or the purchase of contents and regeneration are performed by the approach of storing data in an internal memory through storages, such as a memory card, and CD, DVD.

[0003] In information machines and equipment, such as a cellular phone, a data regenerative apparatus, a game device, and PC, it has an interface for accessing the reception function for receiving negotiation contents from a network, DVD, CD, etc., and has in them RAM, ROM, etc. which are used as a memory area of the control means which is further needed for playback of contents, a program, and data.

[0004] By directions of the user through the input means connected [which were connected and was user-directed] from bodies of information machines and equipment, such as a cellular phone used as a playback device, a data regenerative apparatus, a game device, and PC, various contents, such as music data, image data, or a program, are called from the storage in which built-in or attachment and detachment is free, and

are reproduced through the body of information machines and equipment or the connected display, a loudspeaker, etc.

[0005] Generally as for many software contents, such as a game program, music data, and image data, the right of distribution etc. is held by the implementer and the vender. Therefore, it is common to permit the activity of software, and for reproduction without authorization etc. to be made not to be performed, namely, to take the configuration in consideration of security only to a fixed utilization limit, i.e., a regular user, on the occasion of distribution of these contents.

[0006] One technique of realizing the utilization limit to a user is encryption processing of distribution contents. That is, while distributing various contents, such as voice data enciphered, for example through the Internet etc., image data, and a game program, it is a means, i.e., the configuration which gives a decode key, to decode the distributed encryption contents only to those who were checked as he is a registered user.

[0007] Encryption data can be returned to available decode data (plaintext) by decryption processing in a predetermined procedure. The data encryption and the decryption approach of using an encryption key for encryption processing of such information, and using a decryption key for decryption processing are well learned from the former.

[0008] Although it is seeds, there are various methods currently called the so-called common key encryptosystem-ized method as the one example in the mode of the data encryption and the decryption approach using an encryption key and a decryption key. A common key encryptosystem-ized method gives the encryption key used for data encryption processing, and the common key which uses for these encryption processing and a decryption the decryption key used for a decryption of data as a common thing at the user of normal, and eliminates the data access by the inaccurate user without a key. DES (data code criterion: Deta encryption standard) is in the typical method of this method.

[0009] On the other hand, for example based on a certain password etc., a Hash Function etc. can obtain the encryption key and decryption key which are used for above-mentioned encryption processing and a decryption with the application of a tropism function. On the other hand, it is the function which becomes very difficult [a tropism function] for asking reverse for an input from the output. For example, on the other hand, a tropism function is applied by considering the password which the user decided as an input, and an encryption key and a decryption key are generated based on the output. Thus, the parenchyma top of asking reverse for the password which is data of the original copy becomes impossible from the obtained encryption key and a

decryption key.

[0010] Moreover, the method which made a different algorithm processing with the encryption key used when enciphering, and processing of the decryption key used when decoding is a method called the so-called public-key-encryption-ized method. An unspecified user is the approach of using an usable public key, and a public-key-encryption-ized method performs encryption processing using the public key with which the specific individual published the encryption document to a specific individual. The decode processing of the document enciphered with the public key is attained only with the private key corresponding to the public key used for the encryption processing. Since only the individual who published the public key owns a private key, only an individual with a private key can decode the document enciphered with the public key. A RSA (Rivest-Shamir-Adleman) code is one of the typical things of a public-key-encryption-ized method. By using such a cipher system, the system which enables the decode of encryption contents only to a registered user becomes possible.

[0011]

[Problem(s) to be Solved by the Invention] However, when the contents purchased by the normal purchaser are once decoded, for example, it is copied to removable storage devices, such as a memory card, as it is, set contents storing storage to the device which other users who are the non-purchasers of contents have, and it is reproduced, or it is copied to the storage of further others, and there is possibility of being used for much more users. Thus, the secondary negotiation of disorderly contents may occur based on one normal purchase of contents.

[0012] This invention solves the trouble of such a conventional technique, makes available the contents stored in removable storage devices, such as a memory card, only in the device of the normal purchaser of contents, and aims at preventing setting the contents stored in the memory card etc. to other devices, and being reproduced and used unjustly.

[0013] Furthermore, this invention aims at offering the configuration made available only in the specific playback device by which a normal purchase user has purchase contents in it when removable storage devices, such as a memory card which a user owns, are set, contents are stored in storage and it performs the purchase of contents to the contents distribution terminal which a service provider manages.

[0014]

[Means for Solving the Problem] In the information recording device with which the 1st side face of this invention records information on a record medium The storage means which stored the device node key (DNK) which becomes each node which constitutes the

hierarchy tree structure which used as the leaf the information recording device with which plurality differs from the node key of a proper, and the leaf key of each information recording device proper, It has a cipher-processing means to perform cipher processing of the storing data to said record medium. Said cipher-processing means Cipher processing which applied the cryptographic key (Kcon) to the characteristic value of the specific data regenerative apparatus which reproduces the storing data of said record medium is performed. Generate the cryptographic key (Kst) applied to said storing data, and the storing data encryption processing by this cryptographic key (Kst) generates encryption data:Enc (Kst, DATA). The cryptographic key (Kcon) applied to cipher processing of said characteristic value The cryptographic key data enciphered using the hierarchy tree configuration key stored in the validation key block (EKB) which enciphered the high order key of said hierarchy tree by a low order hierarchy's node key or the key of a leaf key which contains either at least are generated. Said encryption data, It is in the information recording device characterized by having the configuration which performs processing which stores the data file containing said cryptographic key data, and said validation key block (EKB) in said record medium.

[0015] Furthermore, in one embodiment of the information recording apparatus of this invention, said specific data regenerative apparatus is said information recording apparatus itself, and said characteristic value is characterized by being the characteristic value matched with said information recording apparatus.

[0016] In one embodiment of the information recording device of this invention furthermore, said information recording device It is the contents distribution terminal which performs distribution of contents. Said specific data regenerative apparatus It is a data regenerative apparatus using the download contents from said contents distribution terminal. Said characteristic value It is the characteristic value matched with said data regenerative apparatus, and said information recording apparatus is characterized by being the configuration of performing cipher processing which applied said cryptographic key (Kcon) to the characteristic value matched with said data regenerative apparatus inputted from the outside.

[0017] Furthermore, in one embodiment of the information recording apparatus of this invention, characteristic value of said data regenerative apparatus is characterized [at this data regenerative apparatus] by being discernment data of a proper the telephone number or the data regenerative apparatus of a proper.

[0018] Furthermore, in one embodiment of the information recording device of this invention, said record medium is characterized by being a removable removable record medium to said information recording device.

[0019] Furthermore, in one embodiment of the information recording apparatus of this invention, the hierarchy tree configuration key stored in said validation key block (EKB) is characterized by being root key:Kroot set up to the root which is the top-most-vertices node of this hierarchy tree.

[0020] Furthermore, in one embodiment of the information recording apparatus of this invention, the hierarchy tree configuration key stored in said validation key block (EKB) is characterized by being a key acquirable [with decode processing of said validation key block (EKB) by said device node key (DNK)].

[0021] In one embodiment of the information recording apparatus of this invention, furthermore, the hierarchy tree configuration key stored in said validation key block (EKB) It is constituted as a key which can be updated. Said information recording device The updated hierarchy tree configuration key which was stored in the validation key block (EKB) which enciphered the high order key of said hierarchy tree by a low order hierarchy's node key, or the key of a leaf key which contains either at least It is characterized by having the configuration acquired by decode processing of said validation key block (EKB) by said device node key (DNK).

[0022] Furthermore, in one embodiment of the information recording device of this invention, said cipher-processing means is characterized by being the configuration which generates the cryptographic key (Kcon) to the characteristic value of said information recording device based on a random number.

[0023] Furthermore, the 2nd side face of this invention is set to the information regenerative apparatus which performs regeneration of the storing data stored in the record medium. The storage means which stored the device node key (DNK) which becomes each node which constitutes the hierarchy tree structure which used as the leaf the information regenerative apparatus with which plurality differs from the node key of a proper, and a leaf key peculiar to each information ******, It has a cipher-processing means to perform decode processing of the storing data of said record medium. Said cipher-processing means The validation key block (EKB) which enciphered the high order key of said hierarchy tree stored in said record medium by a low order hierarchy's node key or the key of a leaf key which contains either at least is decoded using said device node key (DNK). The hierarchy tree configuration key stored in this validation key block (EKB) is acquired. Acquire a cryptographic key (Kcon) by decode processing of the cryptographic key data enciphered using said hierarchy tree configuration key stored in said record medium, and characteristic value of an information regenerative apparatus own [said] is received. Storing encryption data perform cipher processing which applied said cryptographic key (Kcon), generate the

decode key (Kst) applied to said storing data, and according to this decode key (Kst): Be in the information regenerative apparatus characterized by having the configuration which performs decode processing of Enc (Kst, DATA).

[0024] Furthermore, in one embodiment of the information regenerative apparatus of this invention, characteristic value of said information regenerative apparatus is characterized [at this information regenerative apparatus] by being discernment data of a proper the telephone number or the information regenerative apparatus of a proper.

[0025] Furthermore, in one embodiment of the information regenerative apparatus of this invention, said record medium is characterized by being a removable removable record medium to said information regenerative apparatus.

[0026] Furthermore, in one embodiment of the information regenerative apparatus of this invention, the hierarchy tree configuration key stored in said validation key block (EKB) is characterized by being root key:Kroot set up to the root which is the top-most-vertices node of this hierarchy tree.

[0027] In one embodiment of the information regenerative apparatus of this invention, furthermore, the hierarchy tree configuration key stored in said validation key block (EKB) It is constituted as a key which can be updated. Said information regenerative apparatus The updated hierarchy tree configuration key which was stored in the validation key block (EKB) which enciphered the high order key of said hierarchy tree by a low order hierarchy's node key, or the key of a leaf key which contains either at least It is characterized by having the configuration acquired by decode processing of said validation key block (EKB) by said device node key (DNK).

[0028] Furthermore, the storage means which stored the device node key (DNK) to which the 3rd side face of this invention becomes each node which constitutes the hierarchy tree structure which used as the leaf the information recording device with which plurality differs from the node key of a proper, and the leaf key of each information recording device proper, In the information record approach for said record medium in the information recording device which has a cipher-processing means to perform cipher processing of the storing data to a record medium Cipher processing which applied the cryptographic key (Kcon) to the characteristic value of the specific data regenerative apparatus which reproduces the storing data of said record medium is performed. The step which generates the cryptographic key (Kst) applied to said storing data, the storing data encryption processing by said cryptographic key (Kst) -- encryption data: -- with the step which generates Enc (Kst, DATA) The cryptographic key (Kcon) applied to cipher processing of said characteristic value The step which generates the cryptographic key data enciphered using the hierarchy tree configuration

key stored in the validation key block (EKB) which enciphered the high order key of said hierarchy tree by a low order hierarchy's node key, or the key of a leaf key which contains either at least, and said encryption data, It is in the information record approach characterized by having the step which stores the data file containing said cryptographic key data, and said validation key block (EKB) in said record medium.

[0029] Furthermore, in one embodiment of the information record approach of this invention, said specific data regenerative apparatus is said information recording device itself, and said characteristic value is characterized by being the characteristic value matched with said information recording device.

[0030] In one embodiment of the information record approach of this invention furthermore, said information recording device It is the contents distribution terminal which performs distribution of contents. Said specific data regenerative apparatus It is a data regenerative apparatus using the download contents from said contents distribution terminal. Said characteristic value It is the characteristic value matched with said data regenerative apparatus, and the step which generates said cryptographic key (Kst) is characterized by including the step which performs cipher processing which applied said cryptographic key (Kcon) to the characteristic value matched with said data regenerative apparatus inputted from the outside.

[0031] Furthermore, in one embodiment of the information record approach of this invention, characteristic value of said data regenerative apparatus is characterized [at this data regenerative apparatus] by being discernment data of a proper the telephone number or the data regenerative apparatus of a proper.

[0032] Furthermore, in one embodiment of the information record approach of this invention, said record medium is characterized by being a removable removable record medium to said information recording apparatus.

[0033] Furthermore, in one embodiment of the information record approach of this invention, the hierarchy tree configuration key stored in said validation key block (EKB) is characterized by being root key:Kroot set up to the root which is the top-most-vertices node of this hierarchy tree.

[0034] Furthermore, in one embodiment of the information record approach of this invention, the hierarchy tree configuration key stored in said validation key block (EKB) is characterized by being a key acquirable [with decode processing of said validation key block (EKB) by said device node key (DNK)].

[0035] In one embodiment of the information record approach of this invention, furthermore, the hierarchy tree configuration key stored in said validation key block (EKB) It is constituted as a key which can be updated. Said information record

approach Furthermore, the updated hierarchy tree configuration key which was stored in the validation key block (EKB) which enciphered the high order key of said hierarchy tree by a low order hierarchy's node key, or the key of a leaf key which contains either at least It is characterized by including the step which performs processing acquired by decode processing of said validation key block (EKB) by said device node key (DNK).

[0036] Furthermore, in one embodiment of the information record approach of this invention, said information record approach is characterized by having further the step which generates the cryptographic key (Kcon) to the characteristic value of said information recording device based on a random number.

[0037] Furthermore, the storage means which stored the device node key (DNK) to which the 4th side face of this invention becomes each node which constitutes the hierarchy tree structure which used as the leaf the information regenerative apparatus with which plurality differs from the node key of a proper, and a leaf key peculiar to each information ******, In the information playback approach of performing regeneration of the storing data stored in said record medium in the information regenerative apparatus which has a cipher-processing means to perform decode processing of the storing data of a record medium The validation key block (EKB) which enciphered the high order key of said hierarchy tree stored in said record medium by a low order hierarchy's node key or the key of a leaf key which contains either at least is decoded using said device node key (DNK). The step which acquires the hierarchy tree configuration key stored in this validation key block (EKB), The step which acquires a cryptographic key (Kcon) by decode processing of the cryptographic key data enciphered using said hierarchy tree configuration key stored in said record medium, Cipher processing which applied said cryptographic key (Kcon) is performed to characteristic value of an information regenerative apparatus own [said]. Storing encryption data generate the decode key (Kst) applied to said storing data, and according to this decode key (Kst): Be in the information playback approach characterized by having the step which performs decode processing of Enc (Kst, DATA).

[0038] Furthermore, in one embodiment of the information playback approach of this invention, characteristic value of said information regenerative apparatus is characterized [at this information regenerative apparatus] by being discernment data of a proper the telephone number or the information regenerative apparatus of a proper.

[0039] Furthermore, in one embodiment of the information playback approach of this invention, said record medium is characterized by being a removable removable record medium to said information regenerative apparatus.

[0040] Furthermore, in one embodiment of the information playback approach of this

invention, the hierarchy tree configuration key stored in said validation key block (EKB) is characterized by being root key:Kroot set up to the root which is the top-most-vertices node of this hierarchy tree.

[0041] In one embodiment of the information playback approach of this invention, furthermore, the hierarchy tree configuration key stored in said validation key block (EKB) It is constituted as a key which can be updated. Said information playback approach Furthermore, the updated hierarchy tree configuration key which was stored in the validation key block (EKB) which enciphered the high order key of said hierarchy tree by a low order hierarchy's node key, or the key of a leaf key which contains either at least It is characterized by including the step acquired by decode processing of said validation key block (EKB) by said device node key (DNK).

[0042] Furthermore, the storage means which stored the device node key (DNK) to which the 5th side face of this invention becomes each node which constitutes the hierarchy tree structure which used as the leaf the information recording device with which plurality differs from the node key of a proper, and the leaf key of each information recording device proper, It is the program which makes the information record processing to said record medium in the information recording device which has a cipher-processing means to perform cipher processing of the storing data to a record medium perform on computer system. Said program performs cipher processing which applied the cryptographic key (Kcon) to the characteristic value of the specific data regenerative apparatus which reproduces the storing data of said record medium. The step which generates the cryptographic key (Kst) applied to said storing data, the storing data encryption processing by said cryptographic key (Kst) -- encryption data: -- with the step which generates Enc (Kst, DATA) The cryptographic key (Kcon) applied to cipher processing of said characteristic value The step which generates the cryptographic key data enciphered using the hierarchy tree configuration key stored in the validation key block (EKB) which enciphered the high order key of said hierarchy tree by a low order hierarchy's node key, or the key of a leaf key which contains either at least, and said encryption data, It is in the program characterized by having the step which stores the data file containing said cryptographic key data, and said validation key block (EKB) in said record medium.

[0043] Furthermore, the storage means which stored the device node key (DNK) to which the 6th side face of this invention becomes each node which constitutes the hierarchy tree structure which used as the leaf the information regenerative apparatus with which plurality differs from the node key of a proper, and a leaf key peculiar to each information ******, It can set to the information regenerative apparatus which has

a cipher-processing means to perform decode processing of the storing data of a record medium. It is the program which makes regeneration of the storing data stored in said record medium perform on computer system. Said program The validation key block (EKB) which enciphered the high order key of said hierarchy tree stored in said record medium by a low order hierarchy's node key or the key of a leaf key which contains either at least is decoded using said device node key (DNK). The step which acquires the hierarchy tree configuration key stored in this validation key block (EKB), The step which acquires a cryptographic key (Kcon) by decode processing of the cryptographic key data enciphered using said hierarchy tree configuration key stored in said record medium, Cipher processing which applied said cryptographic key (Kcon) is performed to characteristic value of an information regenerative apparatus own [said]. Storing encryption data generate the decode key (Kst) applied to said storing data, and according to this decode key (Kst): Be in the program characterized by having the step which performs decode processing of Enc (Kst, DATA).

[0044] In addition, the program of this invention is stored in storages, such as the medium offered in a computer-readable format, for example, CD, and FD, MO, to the general purpose computer system which can perform various program codes, for example, and is a program [provide / it / and] which can be offered with transmission media, such as a network, etc.

[0045] Such a program can demonstrate the collaboration-operation on a system and can acquire the same operation effectiveness as other side faces of this invention while it prescribes activation of the various functions which a system has based on reading of a program under processor control.

[0046] The object, the description, and advantage of further others of this invention will become [rather than] clear by detailed explanation based on the example and the drawing to attach of this invention mentioned later. In addition, in this invention, a system is the logical set configuration of two or more equipments, and it does not restrict to what has equipment of each configuration in the same case.

[0047]

[Embodiment of the Invention] The example of a contents distribution system in which the application of the data processing system of this invention to [system outline] drawing 1 is possible is shown. The contents distribution means 10 transmits various contents, such as music, an image, a game, and a program, as encryption data or plaintext (un-enciphering) data to the data-processing means 20. With the data-processing means 20, the contents which received are decoded if needed, and playback of image data and voice data or various programs are performed, and

processing of storing in an internal memory and removable memory is performed. The data exchange between the distribution means 10 of contents and the data-processing means 20 is performed through a memory card, DVD and CD, and other storages through networks, such as the telephone line and the Internet.

[0048] As a contents distribution means 10, there is contents distribution terminal 14 grade which the Internet 11, satellite broadcasting service 12, the telephone line 13, a service provider, etc. installed in the station or the store, in the case of the contents purchase from the contents distribution terminal 14, the removable storage devices 15, such as a memory card, are set to the contents distribution terminal 14, and contents are stored. In addition, in the system of this invention, processing including the encryption processing which gives detail explanation in the latter part in the case of this data migration is performed.

[0049] As a device of the data-processing means 20, there are record regenerators, such as the pocket devices 23, such as a personal computer (PC) 21, the portable device (PD) 22, a cellular phone, and PDA (Personal Digital Assistants), DVD, and a CD player, the game terminal 24, and record regenerative-apparatus 25 grade. Each device of these data-processing means 20 can acquire the contents offered from the contents distribution means 10 from means of communications, other data-processing means, or the data storage means 30, such as a network.

[0050] The memory card (as an example, it is a memory stick (Memory Stick: trademark)) as DVD and CD equipped with storage means, such as a flash memory, and a storage means to have a code processing facility etc. is contained in the data storage means 30.

[0051] Each of the data-processing means 20 can store the purchased contents data in removable storage means, such as an internal memory or a memory card.

[0052] In case contents are outputted and stored in the removable storage means 30 from the internal memory of the data-processing means 20 in the system of this invention, and in case the contents stored in the internal memory of the contents distribution terminal 14 at the time of contents purchase are stored in a removable storage device, processing including encryption processing of the contents explained to a detail in the latter part is performed, and the processing made refreshable only in a just purchaser's device is made.

[0053] The example of migration processing of typical contents data is shown in drawing 2 . The system shown in drawing 2 is drawing explaining possibility that the contents which showed the contents normal purchase terminal 50 and the contents non-normal purchase terminal 60 which is not performing the normal purchase of contents, and

were purchased with the contents normal purchase terminal 50 will be used with the contents non-normal purchase terminal 60 through the removable storage devices 52, such as a memory card (for example, memory stick (Memory Stick: trademark)) which built in rewritable semiconductor memory, such as a flash memory.

[0054] Through networks, such as the Internet, and the telephone line, the contents normal purchase terminal 50 can set a removable storage device 51 to the contents distribution terminal 40, and can purchase contents through processing of storing contents, such as audio data, image data, and a program. These contents are charged contents with which the user who paid the countervalue is provided, or the contents offered for [specific] registered users are contained. In storing ** and contents data, the contents normal purchase terminal 50 performs authentication processing, accounting, etc. between the host computers of a service provider if needed.

[0055] The processing which stores in an internal memory the contents purchased in a regular procedure, and is reproduced is possible for the contents normal purchase terminal 50. Moreover, the processing which stores purchase contents in a removable storage device 52 is also possible, and it is possible to set this to the contents non-normal purchase terminal 60. Moreover, it is also possible to set to the direct contents non-normal purchase terminal 60 the removable storage device 51 to which the contents normal purchase terminal 50 set to the contents distribution terminal 40, and purchased contents.

[0056] In the system of this invention, the contents playback from the removable storage device 52 set to these contents non-normal purchase terminals 60 or a removable storage device 51 is eliminated, and the processing made refreshable only in the contents normal purchase terminal 50 is made.

[0057] In the case of storing of the contents data from the contents normal purchase terminal 50 over the removable storage devices 51 and 52 shown in drawing 2 , or a contents distribution terminal, encryption processing of contents is performed and the processing which enables decode processing of encryption contents only in the contents normal purchase terminal 50 is made. Hereafter, the detail of these processings is explained.

[0058] [the tree(Thurs.) structure as a key distribution configuration] -- the hierarchy tree configuration which offers the configuration which distributes a cipher-processing key with various contents key cryptographic keys for enciphering the cryptographic key applied to cipher processing to the above contents, for example, the contents key applied to cipher processing of contents, and a contents key etc. to the device which has a just license in insurance is explained below using drawing 3 .

[0059] The numbers 0-15 shown in the bottom of drawing 3 are each devices which constitute a data-processing means 20 to perform playback of contents data, and activation, for example, a contents (music data) regenerative apparatus. That is, each leaf (leaf: leaf) of the hierarchy tree(Thurs.) structure shown in drawing 3 is equivalent to each device.

[0060] Each devices 0-15 store in memory the key set which consists of a key (node key) assigned to the node until it reaches [from its own leaf in the time of manufacture or shipment, or the hierarchy tree(Thurs.) structure which sets after that and is shown in drawing 3] the root, and a leaf key of each leaf. These key set is called a device node key (DNK). K0000-K1111 which are shown in the bottom of drawing 3 are the leaf key assigned to each devices 0-15, respectively, and let key:Kroot-K111 indicated by the 2nd knot (node) from the bottom be a node key from Kroot (root key) of the maximum upper case.

[0061] In the tree configuration shown in drawing 3 , a device 0 owns the leaf key K0000, and node key:K000, K00 and K0 and Kroot as a device node key (DNK). A device 5 owns K0101, K010, K01, K0, and Kroot as a device node key (DNK). A device 15 owns K1111, K111, K11, K1, and Kroot as a device node key (DNK). In addition, although shown as a bilateral symmetry configuration in which 16 devices of 0-15 were indicated by the tree of drawing 3 , and the tree structure was also able to take balance of a four-step configuration, it is possible to have a number-of-stages configuration which much more devices are constituted in a tree, and is different in each part of a tree.

[0062] Moreover, the available device is contained in the store various type [, such as a memory card which used the flash memory constituted by various record media, for example, a device embedding mold or the device free / attachment and detachment / for each device contained in the tree structure of drawing 3 , and DVD, CD, MD,]. Furthermore, various application services can live together. The hierarchy tree structure which is the contents or the key distribution configuration shown in drawing 3 after that such a different device and different application constitute [coexistence] is applied.

[0063] In the system by which these various devices and application live together, the part 0, 1, 2, and 3 enclosed with the dotted line of drawing 3 , i.e., devices, is set up as one group using the same record medium. For example, to the device contained in the group enclosed with this dotted line, it collects, common contents are enciphered, and processing in which send the contents key which sends from a provider or is used [each device], or encipher to a provider or a settlement-of-accounts engine too, and the payment data of a contents tariff are outputted to him from each device is performed.

Engines which perform data transmission and reception with each device, such as a content provider or a settlement-of-accounts processing engine, perform the part enclosed with the dotted line of drawing 3 , i.e., the processing which bundles up devices 0, 1, 2, and 3 as one group, and sends data. Two or more such groups exist in the tree of drawing 3 . Engines which perform data transmission and reception with each device, such as a content provider or a settlement-of-accounts processing engine, function as a message data distribution means.

[0064] In addition, a node key and a leaf key are good also as a configuration managed for every group with message data distribution means, such as a provider who may generalize and manage with one certain key management center, and performs various data transmission and reception to each group, and a settlement-of-accounts engine. As for these node keys and a leaf key, in leakage of a key etc., an update process is performed, and a key management center, a provider, a settlement-of-accounts engine, etc. perform this update process.

[0065] In this tree structure, three devices 0, 1, 2, and 3 contained in one group hold the keys K00 and K0 common as a node key, and Kroot so that clearly from drawing 3 . By using this node key share configuration, it becomes possible to provide only devices 0, 1, 2, and 3 with a common contents key. For example, if node key K00 the very thing held in common is set up as a contents key, setting out of a contents key common only to devices 0, 1, 2, and 3 is possible, without performing new key sending. Moreover, if the value Enc (K00, Kcon) which enciphered the new contents key Kcon by the node key K00 is stored in a record medium through a network and distributed to devices 0, 1, 2, and 3 Only devices 0, 1, 2, and 3 become possible [solving Code Enc (K00 Kcon) using the share node key K00 held in each device, and obtaining contents key:Kcon]. In addition, it is shown that Enc (Ka, Kb) is data which enciphered Kb by Ka.

[0066] Moreover, the key which a device 3 owns in t at a certain event: When it is revealed that K0011, K001, K00, K0, and Kroot were analyzed by the aggressor (hacker), and it was exposed of Kroot, in order to protect the data transmitted and received by the system (group of devices 0, 1, 2, and 3) after it, it is necessary to separate a device 3 from a system. For that purpose, a node key: It is necessary to update K001, K00, K0, and Kroot to respectively new key K (t)001 and K (t)00 and K (t)0 and K(t) root, and to tell the updating key to devices 0, 1, and 2. Here, it is shown that K(t) aaa is the updating key of generation (Generation):t of Key Kaaa.

[0067] Distribution processing of an updating key is explained. Renewal of a key is performed by storing the block data called the validation key block (EKB:Enabling Key Block) shown in drawing 4 (A) in a record medium through a network, and supplying it

to each device. A validation key block (EKB) is constituted by the data which enciphered the updating key. A validation key block (EKB) may be called the renewal block of a key (KRB:Key Renewal Block).

[0068] The validation key block (EKB) shown in drawing 4 is EKB which has the data configuration which can be decoded using the device node key (DNK) of the processing possibility of, i.e., self, only in the required device of renewal of a node key. In the devices 0, 1, and 2 in the tree structure shown in drawing 3 , the example of drawing 4 is the block data formed for the purpose of distributing Generation's t updating node key, and has the data configuration which can be decoded using each device node key (DNK) which devices 0, 1, and 2 have. K (t)00 and K (t)0 and K(t) root are acquired by decode processing of a validation key block (EKB) as an updating node key, and, as for a device 0 and a device 1, K (t)001 and K (t)00 and K (t)0 and K(t) root are acquired as an updating node key, as for a device 2.

[0069] For example, as shown in EKB of drawing 4 (A), two or more cryptographic keys are contained in EKB. The cryptographic key of the bottom is Enc (K0010, K(t)001). this -- a device -- two -- having -- a leaf -- a key -- K -- 0010 -- enciphering -- having had -- updating -- a node -- a key -- K -- (-- t --) -- 001 -- it is -- a device -- two -- self -- having -- a leaf -- a key -- this cryptographic key -- decoding -- K -- 001 can be obtained. moreover, K obtained by decode -- 001 -- using -- decode of the 2nd step of cryptographic key Enc (K (t)001 and K (t) -- 00) is possible from under drawing 4 (A) -- becoming -- the updating node key K -- 00 can be obtained. the following -- one by one -- the 2nd step from drawing 4 (A) of cryptographic key Enc (K (t)00 and K (t) -- 0) -- decoding -- the updating node key K -- the 1st step of cryptographic key Enc (K (t)0, K(t) root) is decoded from on 0 and drawing 4 (A), and K(t) root is obtained. On the other hand, it is not contained in the object for which device K0000.K0001 update the node key K000, but the things which are need as an updating node key are K (t)00 and K (t)0 and K(t) root. Device K0000.K0001 decode the 3rd step of cryptographic key Enc (K000, K(t)00) from on drawing 4 (A), and acquire K(t)00. the 2nd step from the following and drawing 4 (A) of cryptographic key Enc (K (t)00 and K (t) -- 0) -- decoding -- the updating node key K -- the 1st step of cryptographic key Enc (K (t)0, K(t) root) is decoded from on 0 and drawing 4 (A), and K(t) root is obtained. Thus, devices 0, 1, and 2 can obtain updated key K (t)001 and K (t)00 and K (t)0 and K(t) root. In addition, the index of drawing 4 (A) shows the absolute address of the node key used as a decode key, and a leaf key.

[0070] The node key of the high-order stage of a tree structure shown in drawing 3 : It is unnecessary, and renewal of K (t)0 and K(t) root can distribute updating node key K(t)00 to devices 0, 1, and 2 by using the validation key block (EKB) of drawing 4 (B),

when only the node key K00 needs to be updated.

[0071] EKB shown in drawing 4 (B) is available when distributing the new contents key shared in a specific group. As an example, the record medium with the devices 0, 1, 2, and 3 in the group who shows by the dotted line is used for drawing 3 , and new common contents key K(t) con presupposes that it is required. this -- the time -- a device -- zero -- one -- two -- three -- being common -- a node -- a key -- K -- 00 -- having updated -- K -- (-- t --) -- 00 -- using -- being new -- being common -- updating -- contents -- a key -- : -- K -- (-- t --) -- con -- having enciphered -- data -- Enc (K (t) 00 K(t) con) -- drawing 4 -- (-- B --) -- being shown -- EKB -- distributing . By this distribution, it becomes possible for a device 4 etc. to distribute as data which are not decoded in other groups' device.

[0072] namely, -- a device -- zero -- one -- two -- EKB -- processing -- having obtained -- K -- (-- t --) -- 00 -- using -- the above -- a cipher -- decoding -- if -- t -- an event -- contents -- a key -- K -- (-- t --) -- con -- obtaining -- things -- possible -- becoming .

[0073] Processing of the device 0 which received EKB shown in the data Enc (K (t) 00 K(t) con) which enciphered new common contents key K(t) con to [distribution of contents key which used EKB] drawing 5 , using K(t)00 as an example of processing which obtains contents key K(t) con in t event, and drawing 4 (B) through the record medium is shown. That is, it is the example which set the encryption message data based on EKB to contents key K(t) con.

[0074] As shown in drawing 5 , a device 0 generates node key K(t)00 by same EKB processing with having mentioned above using the node key K000 which EKB and the them at the generation:t event stored in the record medium store beforehand. Furthermore, updating contents key K(t) con is decoded using updating node key K(t)00 decoded, and in order to use it behind, it enciphers and stores by the leaf key K0000 which he has.

[0075] The example of a format of a validation key block (EKB) is shown in [format of EKB] drawing 6 . A version 601 is an identifier which shows the version of a validation key block (EKB). In addition, a version has the function which shows the response relation of the function and contents which identify the newest EKB. A depth shows the number of hierarchies of the hierarchy tree to the device of the distribution place of a validation key block (EKB). A data pointer 603 is a pointer in which the location of the data division in a validation key block (EKB) is shown, and the tag pointer 604 is a pointer which the location of the tag section and the signature pointer 605 show the location of a signature.

[0076] Data division 606 store the data which enciphered the node key updated, for example. For example, each cryptographic key about the updated node key as shown in

drawing 5 etc. is stored.

[0077] The tag section 607 is a tag in which the physical relationship of the enciphered node key which was stored in data division and a leaf key is shown. The grant rule of this tag is explained using drawing 7 . Drawing 7 shows the example which sends the validation key block (EKB) previously explained by drawing 4 (A) as data. The data at this time come to be shown in the table (b) of drawing 7 . Let the address of the top node contained in the cryptographic key at this time be a top node address. In this case, since updating key K(t) root of a root key is contained, a top node address serves as Kroot. The data Enc (K (t)0, K(t) root) at this time, for example, the maximum upper case, are in the location shown in the hierarchy tree shown in (a) of drawing 7 . here, the following data are Enc (K (t)00 and K (t) -- 0), and are in the location at the lower left of front data on a tree. A tag is set up, and 1 is set up when there are data, and there is nothing, 0 and. A tag is set up as {a left (L) tag and a right (R) tag}. Since there are data in the left of the data Enc (K (t)0, K(t) root) of the maximum upper case and there are no data in L tag =0 and the right, it is set to R tag =1. Hereafter, a tag is set as all data and the data stream shown in drawing 7 (c) and a tag train are constituted.

[0078] A tag is set up in order to show where [of a tree structure] Data Enc (Kxxx, Kyyy) are located. the key data Enc (Kxxx, Kyyy) stored in data division -- since ... is only enumeration data of the key enciphered simply, it enables distinction of the location on the tree of the cryptographic key stored as data with the tag mentioned above. The node index to which encryption data were made to correspond like a configuration of that previous drawing 4 explained is used, without using the tag mentioned above, for example, it is 0:Enc (K (t)0, K(t) root).

00:Enc(K(t)00,K(t)0

000:Enc(K((t)000,K(T)00)

...

** -- although considering as a data configuration [like] is also possible, in the distribution which it will become redundant data and the amount of data will increase if it is a configuration using such an index, and minds a network, it is not desirable. On the other hand, distinction of a key position is attained by the small amount of data by using the tag mentioned above as index data in which a key position is shown.

[0079] It returns to drawing 6 and an EKB format is explained further. A signature (Signature) is electronic signature which published the validation key block (EKB) and which a key management center, contents ROBAIDA, a settlement-of-accounts engine, etc. perform, for example. It checks that the device which received EKB is the validation key block (EKB) which the just validation key block (EKB) publisher published by

signature verification.

[0080] Although the [distribution of contents key and contents which used EKB] above-mentioned example explained the example which sends only a contents key with EKB, the configuration which sends collectively the contents enciphered by the contents key, the contents key enciphered by the contents key code key, and the contents key code key enciphered by EKB is explained below.

[0081] This data configuration is shown in drawing 8 . In the configuration shown in drawing 8 (a) Enc (Kcon, content)801 It is data which enciphered contents (Content) by the contents key (Kcon). Enc (KEK, Kcon)802 It is data which enciphered the contents key (Kcon) by the contents key code key (KEK:Key Encryption Key). Enc (EKB, KEK)803 It is shown that it is data which enciphered the contents key code key KEK by the validation key block (EKB).

[0082] Here, the contents key code key KEK may be the node key (K000, K00 --) shown by drawing 3 , or the root key (Kroot) itself, and may be a key enciphered by the node key (K000, K00 --) or the root key (Kroot).

[0083] Drawing 8 (b) can be considered as the configuration which adds the data in which the link place linked to Enc (EKB, KEK) is shown to each data in such a configuration that two or more contents are recorded on media, and shows the example of a configuration in the case of using Enc (EKB, KEK)805 with the same each, without adding the same Enc (EKB, KEK) as each data.

[0084] drawing 9 -- contents -- a key -- a code -- a key -- KEK -- drawing 3 -- being shown -- a node -- a key -- K -- 00 -- having updated -- updating -- a node -- a key -- K -- (-- t --) -- 00 -- ****** -- having constituted -- a case -- an example -- being shown . In this case, noting that RIBOKU (abatement) of the device 3 is carried out by leakage of a key in the group enclosed with the dotted-line frame of drawing 3 Other groups' member, i.e., (a) validation key block shown in drawing 9 to devices 0, 1, and 2, (EKB) (b) Data which enciphered the contents key (Kcon) by the contents key code key (KEK=K00 (t)), (c) By distributing the data which enciphered contents (content) by the contents key (Kcon), devices 0, 1, and 2 can obtain contents.

[0085] The decode procedure in a device 0 is shown in the right-hand side of drawing 9 . A device 0 acquires a contents key code key (KEK=K00 (t)) from the received validation key block first by decode processing using the leaf key K000 which self holds. Next, the contents key Kcon is acquired by the decode by K(t)00, and contents are further decoded by the contents key Kcon. By these processings, a device 0 becomes available about contents. By processing EKB with respectively different procedure also in devices 1 and 2, it becomes possible to acquire a contents key code key (KEK=K00 (t)), and it becomes

possible to use contents similarly.

[0086] Using the set of the leaf key which self holds, and a node key, i.e., a device node key, (DNK), even if other groups' devices 4 and 5 shown in drawing 3 and 6 ·· receive this same data (EKB), they cannot acquire a contents key code key (KEK=K00 (t)). Also in the device [RIBOKU / device / similarly] 3, a contents key code key (KEK=K00 (t)) cannot be acquired, but only the device which has just access becomes possible [decoding and using contents] by the set of the leaf key which self holds, and a node key, i.e., a device node key, (DNK).

[0087] Thus, if delivery of the contents key using EKB is used, it will become possible to distribute the encryption contents whose decode lessened the amount of data and only the just rightful claimant enabled at insurance.

[0088] In addition, although a validation key block (EKB), a contents key, encryption contents, etc. are the configurations which can be distributed to insurance through a network, it is also possible to store a validation key block (EKB), a contents key, and encryption contents in record media, such as DVD and CD, and to provide for a user. In this case, if it constitutes so that the contents key obtained by decode of the validation key block (EKB) stored in the same record medium may be used for decode of the encryption contents stored in the record medium, available distribution processing of encryption contents, i.e., the contents distribution which limited the available user device, will become realizable with a simple configuration only by the leaf key which only a just rightful claimant holds beforehand, and the node key.

[0089] The example of a configuration which stored the validation key block (EKB) in the record medium with encryption contents at drawing 10 is shown. In the example shown in drawing 10 , contents C1-C4 are stored in a record medium, the data which matched the corresponding [to each storing contents]-further validation key block (EKB) are stored, and the validation key block (EKB_M) of Version M is stored further. For example, it is used for EKB_1 generating the contents key Kcon1 which enciphered contents C1, for example, EKB_2 are used for generating the contents key Kcon2 which enciphered contents C2. In this example, the validation key block (EKB_M) of Version M is stored in the record medium, and since contents C3 and C4 are matched with the validation key block (EKB_M), they can acquire the contents key of contents C3 and C4 by decode of a validation key block (EKB_M). Since EKB_1 and EKB_2 are not stored in the disk, it is necessary to acquire EKB_1 [required in order to decode each contents key by the new offer means, for example network distribution, or distribution by the record medium], and EKB_2.

[0090] As [categorization of hierarchy tree structure] **** was carried out, it is possible

to encipher and distribute not only the contents key applied to contents encryption but the authentication key applied to mutual recognition processing, the ICV (Integrity Check Value) generation key applied as an alteration check value generation key of commo data or a program code, data, etc. with a validation key block (EKB) by applying the hierarchy tree structure of drawing 3 which consists of a root key, a node key, and a leaf key. Furthermore, the configuration which classifies the hierarchy tree structure which defines the node key etc. for every category of each device, and performs efficient key update process, cryptographic key distribution, and data distribution is explained below.

[0091] An example of the classification of the category of a hierarchy tree structure to drawing 11 is shown. In drawing 11 , the root key Kroot and 1101 are set to the maximum upper case of a hierarchy tree structure, the node key 1102 is set to the following intermediate stages, and the leaf key 1103 is set to the bottom. Each device holds each leaf key, and a series of node keys and root key from a leaf key to a root key.

[0092] Here, the existing node of the Mth step is set up as a category node 1104 from the maximum upper case as an example. That is, let each of the node of the Mth step be the device setting-out node of a specific category. Let M+1 or less step of node, and a leaf hereafter be the node and leaf about the device contained in the category by making one node of the Mth step into top-most vertices.

[0093] For example, a category [memorandum RISUTEIIKU (trademark)] is set to one node 1105 of the Mth step of drawing 11 , and the node which stands in a row below in this node, and a leaf are set up as the node or leaf containing various devices which used memorandum RISUTEIIKU only for categories. That is, 1105 or less node is defined as the related node of the device defined as the category of a memory stick, and a set of a leaf.

[0094] Furthermore, a low-ranking stage can be set up as a subcategory node 1106 by several steps from M steps. For example, the node of [the vessel only for playbacks] is set up as a subcategory node contained in the category of the device which used the memory stick for the node under two steps of the category [memory stick] node 1105 as shown in drawing. furthermore -- sub -- a category -- a node -- it is -- playback -- dedication -- a vessel -- a node -- 1106 -- less than -- playback -- dedication -- a vessel -- a category -- containing -- having -- music -- a regenerative function -- with -- a telephone -- a node -- 1107 -- setting up -- having -- further -- the -- low order -- music -- a regenerative function -- with -- a telephone -- a category -- containing -- having -- [-- PHS --] -- a node -- 1108 -- [-- a cellular phone --] -- a node -- 1109 -- it can set up . The device corresponding to the leaf connected to the low order of the [PHS] node 1108 and the

[cellular-phone] node 1109 is usable PHS or a cellular phone about a memory stick.

[0095] Furthermore, a category and a subcategory can be set up in units (these are generically called an entity hereafter) of arbitration, such as not only the class of device but the node which a certain manufacturer, a content provider, a settlement-of-accounts engine, etc. manage uniquely, for example, i.e., a batch, a jurisdiction unit, or an offer service unit. For example, if it sets up as a top-most-vertices node only for game device XYZ(s) to which a game equipment manufacturer sells one category node To the game device XYZ which a manufacturer sells, the node key of the lower berth below the top-most-vertices node, It becomes possible to store and sell a leaf key. Distribution of after that and encryption contents, Or the validation key block (EKB) constituted by the node key below the top-most-vertices node key and the leaf key in distribution of various keys and an update process is generated and distributed, and distribution of available data is attained only to the device below a top-most-vertices node.

[0096] Thus, by making one node into top-most vertices, carrying out it, and considering as the configuration which sets up the following nodes as a related node of the category defined as the top-most-vertices node, or a subcategory The validation key block (EKB) to which the manufacturer who manages one top-most-vertices node of a category stage or a subcategory stage, a content provider, etc. make the node top-most vertices is generated uniquely. The configuration distributed to the device belonging to below a top-most-vertices node is attained, and renewal of a key can be performed, without affecting at all the device belonging to the node of other categories which do not belong to a top-most-vertices node.

[0097] [-- simple -- key distribution configuration] by EKB -- for example, when [which was explained previously] sending a key, for example, a contents key, to a predetermined device (leaf) in the tree configuration of drawing 3 , the validation key block (EKB) which can be decoded is generated and offered using the leaf key and node key which the key distribution place device owns. For example, in the tree configuration shown in drawing 12 (a), when transmitting a key, for example, a contents key, to the devices a, g, and j which constitute a leaf, the validation key block (EKB) which can be decoded is generated and distributed in each node of a, g, and j.

[0098] For example, encryption processing of the contents key K(t) con is carried out by updating root key K(t) root, and the case where it distributes with EKB is considered. In this case, using the leaf and node key which each shows to drawing 12 (b), processing of EKB is performed, decode processing of contents key K(t) con is performed by updating root key K(t) root which acquired and acquired K(t) root, and, as for Devices a, g, and j, a contents key is obtained.

[0099] In this case, the configuration of the validation key block (EKB) offered comes to be shown in drawing 13 . The validation key block (EKB) shown in drawing 13 is constituted according to a format of the validation key block (EKB) explained by previous drawing 6 , and has data (cryptographic key) and a corresponding tag. if a tag has data in the left (L), the right (R), and each direction as previously explained using drawing 7 -- 0 -- 1 is shown if there is nothing.

[0100] Based on the cryptographic key and tag of a validation key block (EKB), the device which received the validation key block (EKB) performs decode processing of a cryptographic key one by one, and acquires the updating key of a host node. As shown in drawing 13 , the validation key block (EKB) increases the amount of data, so that there are many number of stageses (depth) from the root to a leaf. A number of stages (depth) increases according to the number of devices (leaf), and when there are many devices used as the distribution place of a key, the amount of data of EKB will increase further.

[0101] The configuration which enabled the cutback of the amount of data of such a validation key block (EKB) is explained. Drawing 14 shows the example which simplified and constituted the validation key block (EKB) according to the key distribution device.

[0102] The case where a key, for example, a contents key, is transmitted like drawing 13 to the devices a, g, and j which constitute a leaf is assumed. As shown in (a) of drawing 14 , the tree constituted only by the key distribution device is built. In this case, based on the configuration shown in drawing 12 (b), the tree configuration of drawing 14 (b) is built as a new tree configuration. That Kj does not have branching from Kroot and only one branch should exist, in order to result [from Kroot] in Ka and Kg, the tree of drawing 14 (a) of the dichotomy configuration only from only constituting the branch point in K0 is built.

[0103] As shown in drawing 14 (a), the simplified tree which has only K0 as a node is generated. The validation key block (EKB) for updating key distribution is generated based on these simple trees. The tree shown in drawing 14 (a) is a reconstruction hierarchy tree reconstructed by choosing the pass which constitutes the dichotomy mold tree which made the bottom the end node or leaf which can decode a validation key block (EKB), and omitting an unnecessary node. The validation key block (EKB) for updating key distribution is constituted only based on the key corresponding to the node or leaf of this reconstruction hierarchy tree.

[0104] Although the data which enciphered all the keys until the validation key block (EKB) explained by previous drawing 13 results [from each leaves a, g, and j] in Kroot were stored, Simplification EKB stores the encryption data only about the node which

constitutes the simplified tree. As shown in drawing 14 (b), a tag has a triplet configuration. if it has the 1st and the 2nd bit of the example of drawing 13 and the same semantics and there are data in the left (L), the right (R), and each direction -- 0 -- 1 is shown if there is nothing. The 3rd bit is a bit to show whether the cryptographic key is stored in EKB, and when data are stored and there are not 1 and data, it is set up as 0.

[0105] As the validation key block (EKB) with which is stored in a data communication network or a storage, and a device (leaf) is provided was shown in drawing 14 (b), as compared with the configuration shown in drawing 13 , the amount of data was reduced substantially. Each device which received the validation key block (EKB) shown in drawing 14 can realize decode of a predetermined cryptographic key by carrying out the sequential decode only of the data of a part with which 1 was stored in the 3rd bit of a tag. For example, Device a decodes the encryption data Enc (Ka, K(t)0) by the leaf key Ka, acquires node key K(t)0, by node key K(t)0, decodes the encryption data Enc (K (t)0, K(t) root), and acquires K(t) root. Device j decodes the encryption data Enc (Kj and K(t) root) by the leaf key Kj, and acquires K(t) root.

[0106] Thus, by generating a validation key block (EKB) only using the key of the leaf which builds the simplified new tree configuration which is constituted only by the device of a distribution place, and constitutes the built tree, and a node, it becomes possible to generate the validation key block (EKB) of the small amount of data, and activation of data distribution of a validation key block (EKB) is attained efficiently.

[0107] In addition, the simplified hierarchy tree configuration is effectively utilizable especially in the EKB management configuration of the entity unit explained in the latter part. Entities are two or more nodes chosen from the node or leaf which constitutes the tree configuration as a key distribution configuration, or the aggregate block of a leaf. An entity is a set set up according to the class of device, or is set up as a set of various modes, such as batches with a certain common feature, such as management units, such as a device offer manufacturer, a content provider, and a settlement-of-accounts engine, a jurisdiction unit, or an offer service unit. The devices classified into a certain common category have gathered for one entity, for example, the generation of the simplified validation key block (EKB) which can be decoded, and distribution are attained in the device belonging to the selected entity by reconstructing the simplified same tree with having mentioned above by the top-most-vertices node (subroot) of two or more entities, and generating EKB. The latter part explains the management configuration of an entity unit to a detail.

[0108] In addition, such a validation key block (EKB) can be considered as the configuration stored in information record media, such as an optical disk and DVD. For

example, the configuration which provides each device with the information record medium which stored further message data, such as contents enciphered by the updating node key, in the validation key block (EKB) containing the data division constituted with above-mentioned cryptographic key data and the tag section as identification-of-position data in a cryptographic key data-hierarchy tree structure is possible. According to the discernment data of the tag section, a device carries out a sequential extract, and decodes the cryptographic key data contained in a validation key block (EKB), and it becomes possible to acquire a key required for decode of contents and to use contents. Of course, it is good also as a configuration which distributes a validation key block (EKB) through networks, such as the Internet.

[0109] In [data logging and regeneration] to a removable record medium, next the processing configuration which applied the validation key block (EKB) which applied the hierarchy tree configuration mentioned above, the data storage processing to memory cards, such as the record medium which can be detached and attached freely (removable storage device), for example, a memory stick etc., is explained to PC as equipment which performs contents playback, a cellular phone, and a regenerative apparatus.

[0110] (An information recording device and information regenerative-apparatus configuration) Drawing 15 is the block diagram showing the example of a configuration of the data processor as the information recording device which performs record or regeneration of contents, and an information regenerative apparatus. It is PC, a cellular phone, a data regenerative apparatus, etc., and, specifically, the removable storage device as record media, such as a memory card, has a removable configuration.

[0111] A data processor 100 The radial transfer of a digital signal I/O I/F (Interface)120 to perform, A/D which performs radial transfer of an analog signal, I/O I/F (Interface)130 equipped with D/A converter 131, the cipher-processing means 140, ROM () [Read Only] It has the drive 190 of Memory150, RAM (Random Access Memory)160, CPU (Central Processing Unit)170, an internal memory 180, and a removable storage device 200. These are mutually connected by the bus 110.

[0112] I/O I/F120 receives the digital signal on a bus 110, and outputs it outside while it receives the digital signal which constitutes various contents, such as an image supplied from the outside, voice, and a program, and outputs it on a bus 110. I/O I/F130 builds in A/D and D/A converter 131. The analog signal as contents supplied from the outside is received, and I/O I/F130 is carrying out A/D (Analog Digital) conversion by A/D and D/A converter 131, it receives the digital signal on a bus 110 while outputting it on a bus 110 as a digital signal, it is carrying out D/A (Digital Analog) conversion by A/D and D/A

converter 131, and outputs it outside as an analog signal.

[0113] A cipher-processing means 140 enciphers or decodes the digital signal as contents which consist of LSI (Large Scale IntegratedCurcuit) of for example, one chip, for example, are supplied through a bus 110, and has the configuration which performs various processings accompanying cipher processing, such as processing outputted on a bus 110, and processing which generates the cipher-processing key based on the random number which generated the random number and was generated. In addition, the cipher-processing means 150 is possible not only for the 1 chip LSI but the thing which the configuration which combined various kinds of software or hardware realizes, and good also as a configuration performed by the function of CPU170.

[0114] ROM150 stores the fixed data as the program which CPU170 performs, or an operation parameter. RAM (Random Access Memory)160 is used as the storage area of the program performed in processing of CPU170, and the parameter which changes suitably in program manipulation, and a work-piece field. CPU170 performs the program stored in ROM150 and the internal-memory 180 grade, and performs control of cipher processing by the cipher-processing means 150, and the various processings accompanying record playback of data.

[0115] Store I/F190 supplies and records the data supplied through a bus 110 on a removable storage device 200 while it reads data from a removable storage device 200 (reproducing) and outputs them on a bus 110 by controlling data I/O of as opposed to the removable storage device 200 in which an account rec/play student is possible for digital data.

[0116] This data processor corresponds to the leaf of a tree configuration explained using drawing 3 , and the device node key (DNK) as a key set which consists of a leaf key and a node key is stored in an internal memory 180. For example, if it is a data processor corresponding to a device 0, it stores in an internal memory 180 by using the leaf key K0000, and node key:K000, K00 and K0 and Kroot as a device node key (DNK). In addition, the internal memory 180 is usable also as the storing field of the contents inputted from the outside through I/O I/F120,140 or storage I/F, and a storing field of a validation key block (EKB).

[0117] The data processor shown in drawing 15 purchases contents from a network, the telephone line, or a contents distribution terminal to normal, stores them in an internal memory 180, and regenerates by reading contents from an internal memory 180. It reproduces, after performing decode processing of EKB by the device node key (DNK) stored in equipment and decoding encryption contents by the acquired contents key, as previously explained using drawing 9 if it is the contents as which the contents offered

were enciphered using the contents key Kcon acquirable [with processing of the above-mentioned validation key block (EKB)] from the outside.

[0118] such contents -- in a refreshable data processor, it acquires from the exterior and the processing in the case of outputting the contents stored in the internal memory to the memory card as a removable storage device is explained.

[0119] (Contents storing processing) Drawing which explains the procedure of the contents storing processing to the removable storage device in a data processor to drawing 16 is shown. The example shown in drawing 16 is an example of processing in case a data processor is equivalent to the device 0 in the tree configuration of drawing 3 .

[0120] First, a data processor chooses EKB corresponding to the contents stored in the removable storage device as a data-logging medium, performs decode processing of EKB using the device node key (DNK) of self, and takes out the root key which is a hierarchy tree configuration key from EKB. In the example of drawing, EKB corresponding to the contents stored in a removable storage device is EKB of version:t, and a data processor acquires EKB of version:t from an internal memory, performs decode of EKB using K000 in a device node key and this case, and takes out root key K(t) root.

[0121] Next, a data processor generates a random number and generates contents key:Kcon based on a random number. In case this contents key stores contents to a removable storage device, based on the random number generated serially, a different contents key for every storing processing of contents will be generated. In addition, it is processing for carrying out to generation processing of this contents key being applicable also when the contents acquired from the network or the contents distribution terminal are not enciphered using the contents key. It is the case where the contents acquired from the exterior are beforehand enciphered by the contents key, and when a contents key can be acquired from the exterior, the generation processing of a contents key based on this random number may be omitted, and may apply the contents key acquired from the exterior. In addition, even if it is this case, based on a random number, a contents key may be anew generated within a data processor.

[0122] Next, encryption data encipher by root key:K(t) root which acquired previously the contents key generated, for example based on the random number by EKB processing, and according to the root key of a contents key: Acquire Enc (K(t) root, Kcon).

[0123] Furthermore, if ID of a data processor, for example, a data processor, is a cellular phone by generated contents key:Kcon, the telephone number corresponding to a cellular phone will be enciphered, and Enc (Kcon, ID) will generate storage key:Kst.

[0124] Next, the storage key generated by enciphering ID by contents key:Kcon: Encipher contents (DATA) using Kst and generate encryption contents:Enc (Kst, DATA).

[0125] thus, generated contents key: -- root key [of Kcon]: -- encryption data: by K(t) root -- let Enc (K(t) root, Kcon) and encryption data:Enc (Kst, DATA) by storage key:Kst of contents (DATA) be the storing data files to a removable storage device.

[0126] A data processor combines the data file containing these encryption contents, and a corresponding EKB file, and stores them in a removable storage device. In addition, the EKB file and data file to store store by carrying out mutual matching. Matching can be performed by adding the version information of EKB to the data file stored, for example. As previous drawing 6 explained, version information is beforehand added to the EKB file.

[0127] The example of a configuration of an EKB file and a data file stored in drawing 17 at a removable storage device is shown. An EKB file is EKB which can acquire root key:K(t) root which is a hierarchy tree configuration key using the device node key (DNK) beforehand distributed to the data processor. Moreover, encryption data based on encryption data:Enc (K(t) root, Kcon) according to root key:K(t) root of contents key:Kcon as the data file was explained using drawing 16 , and storage-key:Kst of contents (DATA): In the case of EKB version information and the example of this drawing, it has the composition that version:t was recorded, including Enc (Kst, DATA). Two or more contents may be stored in a removable storage device, and the EKB file corresponding to each is also collectively stored in it.

[0128] (Data regeneration) The processing in the case of reproducing the encryption contents (DATA) stored in such a removable storage device (record medium) is explained using drawing 18 .

[0129] The example of processing of drawing 18 is a just contents purchaser, is contents regeneration in the data processor (device 0) which performed contents storing processing to the removable storage device, and shows the example to which normal contents regeneration is carried out.

[0130] First, a data processor acquires the EKB version information which corresponds from the data file stored in the removable storage device, in the acquired version information and this example, performs decode processing of EKB using the device node key (DNK) which acquired the EKB file corresponding to a version (t) from the removable storage device, and was stored in the data processor, and acquires root key:K(t) root which is a hierarchy tree configuration key. Succeeding in this EKB decode processing becomes only the device which stored beforehand the device node key (DNK) which can decode EKB.

[0131] Next, a data processor performs decode processing which applied data:K[root key / which acquired Enc (K(t) root, Kcon) and was acquired by EKB processing /:] (t)

root which enciphered contents key:Kcon by root key:K(t) root from the data file in a removable storage device, and acquires contents key:Kcon.

[0132] Next, if a data processor is a cellular phone and a data processor is a regenerative apparatus of the telephone number or others, it will carry out encryption:Enc (Kcon, ID) of ID, such as an equipment item number, with the application of acquired contents key:Kcon, and will generate storage key:Kst. This storage key: The storage key from which Kst differs for every device based on self ID will be generated. That is, when a storage key is generated in other devices with other ID, a different storage key is generated.

[0133] Next, the storage key which the data processor took out encryption data:Enc (Kst, DATA) by storage-key:Kst of contents (DATA) from the data file in a removable storage device, and was generated: Perform decode processing using Kst. The storage key applied to encryption on the occasion of the contents storing processing to a removable storage device in order to succeed in this decode processing: The same storage key as Kst needs to be generated. In the case of the example shown in this drawing 18 , a data processor is a device 0, and it is the device which stored the contents to a removable storage device, and since ID is the same, generation of the same storage key as the time of data storage is performed, and it succeeds in decode of encryption contents:Enk (Kst, DATA), and becomes reproducible [contents].

[0134] Even if it is going to perform data playback in the device which performed storing processing of contents to the removable storage device, and a different device, it will differ from the storage key which ID differed and the storage key generated applied at the time of data storage, and decode of encryption contents:Enk (Kst, DATA) cannot be performed, but playback of contents becomes impossible.

[0135] Thus, according to the configuration of this invention, it is needed that it is the device which can acquire the contents key which can be decoded by EKB processing as an execution condition of the contents playback stored in the removable storage device, and that it is the same device which performed record processing further. Therefore, it belongs to the specific group of the tree configuration shown in drawing 3 , and even if it is the case where two or more devices which can decode the same EKB exist, a refreshable device becomes possible [limiting to the only device which stored contents in the removable storage device] about the contents stored in the removable storage device.

[0136] (Contents download processing in a contents distribution terminal) Although the data processor explained the contents beforehand stored in the internal memory supposing the processing stored in a removable storage device, the contents storing

processing mentioned above For example, a service provider provides and a user sets a removable storage device to the distribution terminal of contents installed in the station, the store, etc. the removable storage device after purchasing namely, downloading contents -- a self data processor (PC --) Also when it is going to set in a cellular phone, a regenerative apparatus, etc. and is going to reproduce contents, in the device which purchased contents, a refreshable configuration is realized like above-mentioned processing.

[0137] A user sets the removable storage device as a record medium to the distribution terminal of contents using drawing 19 , and the processing which purchases contents is explained.

[0138] A service provider provides and a regenerative apparatus B and 500 are indicated to be the regenerative apparatus A of the cellular-phone mold as a data processor and 400 which are going to purchase contents from the distribution terminal 300 of contents installed in the station, the store, etc., and the distribution terminal 300 of contents, and are going to perform playback to drawing 19 . A regenerative apparatus A, 400, and a regenerative apparatus B and 500 choose the contents which have set a removable storage device 600 like a memory card to the contents distribution terminal 300, and it performs purchase, i.e., the processing which downloads selection contents to a removable storage device 600.

[0139] The configuration of the contents distribution terminal 300 is explained. A contents distribution terminal stores in the storage means 370 the device node key (DNK) which is set up as a data processor (device) corresponding to one leaf of a tree configuration explained using [else / drawing 3] previously, and is set as a response leaf, and has a configuration with the removable removable storage devices 600, such as a memory card.

[0140] The contents distribution terminal 300 has I/O I/F (Interface)320 which performs data radial transfer, the cipher-processing means 330, ROM (Read Only Memory)340, RAM (Random Access Memory)350 and CPU (Central Processing Unit)360, the storage means 370, and removable storage device I/F (Interface)380, and these are mutually connected by the bus.

[0141] I/O I/F320 displays downloadable contents information, price information, etc., and processes the data input accompanying the contents purchase processing from a user. The cipher-processing means 330 enciphers or decodes the digital signal as contents which consist of LSI (Large Scale IntegratedCurcuit) of for example, one chip, for example, are supplied through a bus, and has the configuration which performs various processings accompanying cipher processing, such as processing outputted on a

bus, and processing which generates the cipher-processing key based on the random number which generated the random number and was generated. In addition, the cipher-processing means 330 is possible not only for the 1 chip LSI but the thing which the configuration which combined various kinds of software or hardware realizes, and good also as a configuration performed by the function of a control means (CPU) 360.

[0142] ROM340 stores the fixed data as the program which a control means (CPU) 360 performs, or an operation parameter. RAM (Random Access Memory)350 is used as the storage area of the program performed in processing of a control means (CPU) 360, and the parameter which changes suitably in program manipulation, and a work-piece field. A control means (CPU) 360 performs the program stored in ROM340 and the storage means 370 grade, and performs control of the various processings accompanying cipher processing by the cipher-processing means 330, and download processing of data.

[0143] Store I/F380 controls the data I/O to a removable storage device 200. This contents distribution terminal 300 corresponds to the leaf of a tree configuration explained using drawing 3 , and the device node key (DNK) as a key set which consists of a leaf key and a node key is stored in the storage means 370. For example, if it is the contents distribution terminal 300 corresponding to a device 0, it stores in the storage means 370 by using the leaf key K0000, and node key:K000, K00 and K0 and Kroot as a device node key (DNK). In addition, the storage means 370 is used also as the storing field of contents, and a storing field of a validation key block (EKB).

[0144] A removable storage device 600 is set to the contents distribution terminal 300 shown in drawing 19 , and the processing in the case of purchasing contents is explained.

[0145] For example, the user who is going to reproduce purchase contents using a regenerative apparatus A and 400 sets to the contents distribution terminal 300 the removable storage device 600 which performs download of contents.

[0146] Next, through I/O I/F320, a contents purchase user specifies contents and inputs the discernment data of a proper into a device for the telephone number as a regenerative apparatus A and ID of 400 etc. further.

[0147] Processing of the contents distribution terminal 300 turns into processing previously explained using drawing 16 , and the almost same processing, and as shown in drawing 17 , an EKB file and a data file are stored in a removable storage device. The data storage processing to the removable storage device 600 of the contents distribution terminal 300 is explained referring to drawing 16 .

[0148] The contents distribution terminal 300 is explained as a thing corresponding to the device 0 in the tree configuration of drawing 3 . In addition, a regenerative apparatus A and 400 are the devices corresponding to one in the tree configuration of

drawing 3 of leaves, and store the device node key (DNK) in the interior.

[0149] First, the contents distribution terminal 300 chooses EKB corresponding to the contents which the user specified through I/O I/F320, performs decode processing of EKB using the device node key (DNK) of self, and takes out the root key which is a hierarchy tree configuration key from EKB. In the example of drawing 16 , EKB corresponding to the contents stored in a removable storage device is EKB of version:t, and the contents distribution terminal 300 acquires EKB of version:t from the storage means 370, performs decode of EKB using K000 in a device node key and this case, and takes out root key K(t) root.

[0150] Next, the contents distribution terminal 300 generates a random number in the cipher-processing means 330, and generates contents key:Kcon based on a random number. In case this contents key stores contents to a removable storage device, based on the random number generated serially, a different contents key for every download processing to the removable storage device of contents will be generated. In addition, it is the case where are processing for making application possible also when contents are not enciphered using the contents key, and, as for generation processing of this contents key, contents are beforehand enciphered by the contents key as mentioned above, and the contents key which omitted the generation processing of a contents key based on this random number, and acquired the contents key from the exterior when it was acquisition ending from the outside may be applied. In addition, even if it is this case, based on a random number, a contents key may be anew generated within the contents distribution terminal 300.

[0151] Furthermore, encryption data encipher by root key:K(t) root which acquired previously the contents key generated based on the random number by EKB processing, and according to the root key of a contents key: Generate Enc (K(t) root, Kcon).

[0152] Furthermore, in the contents purchased equipment inputted by the user through I/O I/F320 by generated contents key:Kcon, and this example, a regenerative apparatus A and the telephone number corresponding to the cellular phone as ID of 400 are enciphered, and Enc (Kcon, ID) generates storage key:Kst.

[0153] Next, the storage key generated by enciphering ID by contents key:Kcon: Encipher contents (DATA) using Kst and generate encryption contents:Enc (Kst, DATA).

[0154] thus, generated contents key: -- root key [of Kcon]: -- encryption data: by K(t) root -- let Enc (K(t) root, Kcon) and encryption data:Enc (Kst, DATA) by storage key:Kst of contents (DATA) be the storing data files to a removable storage device.

[0155] The contents distribution terminal 300 combines the data file containing these encryption contents, and a corresponding EKB file, and stores them in a removable

storage device. In addition, the EKB file and data file to store store by carrying out mutual matching. Matching can be performed by adding the version information of EKB to the data file stored, for example. As previous drawing 6 explained, version information is beforehand added to the EKB file.

[0156] Thus, the storage key which the contents distribution terminal 300 generated storage-key:Kst based on ID inputted from the outside, and was generated: Encipher contents using kst. The configuration of the EKB file stored in a removable storage device and a data file is the same as the configuration of drawing 17 explained previously, and an EKB file and a data file are matched and it is stored.

[0157] Thus, the processing in the case of reproducing the encryption contents (DATA) stored in the removable storage device 600 from the contents distribution terminal 300 is the same as processing of drawing 18 explained previously.

[0158] However, the example of processing of drawing 18 is an example of processing of the device 0 in the device of the tree configuration of drawing 3 . That the contents distribution terminal 300 is equivalent to a device 0, then when it assumes, a regenerative apparatus A and 400 are not the device 0 but the devices 1. In this case that processing The EKB version information which corresponds from the data file stored in the removable storage device is acquired. In the acquired version information and this example, decode processing of EKB is performed using the device node key (DNK) which acquired the EKB file corresponding to a version (t) from the removable storage device, and was stored in a regenerative apparatus A and 400, and root key:K (t) is acquired. The device which stored beforehand the device node key (DNK) which can decode EKB succeeds in this EKB decode processing.

[0159] Next, a regenerative apparatus A and 400 perform decode processing which applied data:K[root key / which acquired Enc (K(t) root, Kcon) and was acquired by EKB processing /:] (t) root which enciphered contents key:Kcon by root key:K(t) root from the data file in a removable storage device, and acquire contents key:Kcon.

[0160] Next, a regenerative apparatus A and 400 carry out encryption:Enc (Kcon, ID) of ID, i.e., the telephone number, by acquired contents key:Kcon, and generate storage key:Kst. This storage key: Kst becomes the same thing as storage key:Kst which the contents distribution terminal 300 generated based on ID inputted by the user at the time of the purchase of contents.

[0161] Next, the storage key which a regenerative apparatus A and 400 took out encryption data:Enc (Kst, DATA) by storage-key:Kst of contents (DATA) from the data file in a removable storage device, and was generated: Perform decode processing using Kst. The storage key applied to encryption on the occasion of the contents storing

processing to a removable storage device in order to succeed in this decode processing: The same storage key as Kst needs to be generated. In this case, since ID applied at the time of storing of contents and playback is a regenerative apparatus A and the telephone number of 400 and its ID is the same, generation of the same storage key as the time of data storage is performed, and it succeeds in decode of encryption contents:Enk (Kst, DATA), and becomes reproducible [contents].

[0162] When it is going to perform data playback in the device which performed storing processing of contents to the removable storage device, and a different device, For example, even if the regenerative apparatus B shown in drawing 19 and 500 tend to borrow a removable storage device 600, tend to set to a regenerative apparatus B and 500 and tend to perform playback The storage key which a storage key will be generated based on ID (for example, equipment item number) which is different in a regenerative apparatus B and 500, and was generated The contents distribution terminal 300 becomes a different thing from the storage key applied when contents were enciphered and stored in a removable storage device 600, decode processing cannot be performed but regeneration becomes impossible.

[0163] Thus, in addition to being the device which can acquire the contents key which can be decoded by EKB processing from an external contents distribution terminal as conditions which perform playback of the contents stored in the removable storage device according to the configuration of this invention, it is further set up as conditions in the case of contents purchase processing that it is the same device as the specified device. Therefore, it belongs to the specific group of the tree configuration shown in drawing 3 , and even if it is the case where two or more devices which can decode the same EKB exist, it becomes possible to limit to the only device with which the refreshable device specified the contents stored in the removable storage device at the time of contents purchase.

[0164] (Contents record, regeneration sequence) Next, procedure is explained using a flow about storing processing of the contents to a removable storage device, and regeneration of the contents stored in the removable storage device.

[0165] First, according to the processing flow of drawing 20 , the procedure which stores in a removable storage device the contents from which the removable data processor stored the removable storage device in the internal memory is explained.

[0166] First, in step S5001, the EKB file applied to the contents stored in a removable storage device is chosen. Although the data processor should store only the EKB file of the latest version fundamentally, when two or more EKB files are stored, for example, it chooses the newest EKB from those EKB files.

[0167] Next, in step S5002, decode processing of EKB is performed using the device node key (DNK) which is the key set of a leaf key and a node key stored in equipment, and the root key Kroot which is a hierarchy tree configuration key is acquired.

[0168] Next, in step S5003, a random number is generated and contents key:Kcon is generated. In addition, it is processing for carrying out to generation processing of this contents key being applicable also when the contents acquired from the network or the contents distribution terminal are not enciphered using the contents key. It is the case where the contents acquired from the exterior are beforehand enciphered by the contents key, and when a contents key can be acquired from the exterior, the generation processing of a contents key based on this random number may be omitted, and may apply the contents key acquired from the exterior. In addition, even if it is this case, based on a random number, a contents key may be anew generated within a data processor.

[0169] Next, encryption according [in / in step S5004, acquire ID from an internal memory, and / a cipher-processing means] to contents key:Kcon of ID: Perform Enc (Kcon, ID) and generate storage key:Kst (S5005).

[0170] Furthermore, in step S5006, by root key:Kroot acquired by EKB processing, encryption processing of contents key:Kcon is performed and Enc (Kroot, Kcon) is generated.

[0171] Furthermore, in step S5007, encryption processing is performed for the contents (DATA) stored in a removable storage device by storage key:Kst, Enc (Kst, DATA) is generated, an EKB file and the data file which stored Enc (Kroot, Kcon) and Enc (Kroot, Kcon) are matched in step S5008, and it stores in a removable storage device.

[0172] Next, according to the processing flow of drawing 21 , a contents distribution terminal explains the procedure stored in the removable storage device in which the user set contents.

[0173] First, in step S6001, the EKB file applied to the contents specified by [which is stored in the removable storage device which the user set] a user is chosen. Next, in step S6002, decode processing of EKB is performed using the device node key (DNK) which is the key set of a leaf key and a node key stored in equipment, and the root key Kroot which is a hierarchy tree configuration key is acquired.

[0174] Next, in step S6003, a random number is generated and contents key:Kcon is generated. In addition, it is the case where are processing for making application possible also when contents are not enciphered using the contents key, and, as for generation processing of this contents key, contents are beforehand enciphered by the contents key as mentioned above, and the contents key which omitted the generation

processing of a contents key based on this random number, and acquired the contents key from the exterior when it was acquisition ending from the outside may be applied. In addition, even if it is this case, based on a random number, a contents key may be anew generated within a contents distribution terminal.

[0175] Next, encryption according [in / in step S6004, acquire ID inputted by the user from the outside, and / a cipher-processing means] to contents key:Kcon of ID: Perform Enc (Kcon, ID) and generate storage key:Kst (S6005).

[0176] Furthermore, in step S6006, by root key:Kroot acquired by EKB processing, encryption processing of contents key:Kcon is performed and Enc (Kroot, Kcon) is generated.

[0177] Furthermore, in step S6007, encryption processing is performed for the contents (DATA) stored in a removable storage device by storage key:Kst, Enc (Kst, DATA) is generated, an EKB file and the data file which stored Enc (Kroot, Kcon) and Enc (Kroot, Kcon) are matched in step S6008, and it stores in a removable storage device.

[0178] Next, according to the processing flow of drawing 22 , the procedure which reproduces the contents from which the removable data processor stored the removable storage device in the removable storage device is explained.

[0179] First, in step S7001, the EKB file applied to the contents reproduced from a removable storage device is chosen. Selection of an EKB file is performed as processing which acquires the EKB file which is in agreement with the EKB version information added to the data file containing the encryption contents shown in drawing 17 explained previously from a removable storage device. In step S7002, when it succeeds in EKB acquisition, it progresses to degree step, and when EKB cannot be acquired, processing is ended as an error (S7011).

[0180] Next, in step S7003, decode processing of EKB acquired from the removable storage device is performed using the device node key (DNK) which is the key set of a leaf key and a node key stored in equipment, and the root key Kroot which is a hierarchy tree configuration key is acquired. When it succeeds in root key Kroot acquisition, it progresses to degree step, and when the root key Kroot cannot be acquired, processing is ended as an error (S7011). When the root key Kroot is unacquirable, it is the case, RIBOKU [the equipment], etc.

[0181] Next, in step S7005, encryption contents:Enc (Kst, DATA) is read from the storing data file of a removable storage device. From the storing data file of a removable storage device to next, an encryption contents key: Read Enc (Kroot, Kcon), perform decode processing by the root key Kroot acquired by EKB decode processing at step S7003, and obtain the contents key Kcon (S7006).

[0182] Next, encryption by the contents key [on step S7007 and as opposed to self ID]: Perform Enc (Kcon, ID) and generate storage key:Kst. next, in step S7008, decode processing is performed with the application of storage key:Kst which generated encryption contents:Enc (Kst, DATA) in which the removable storage device carried out storing data file reading appearance.

[0183] If judged with decode having succeeded in step S7009, it will reproduce at step S7010. In decode failure, in step S7009, processing is ended as an error (S7011). It becomes an error when the storage key generated based on ID in step S7007 differs from the storage key applied in the contents storing processing to a removable storage device. When ID applied to storage key generation differs, activation of playback becomes impossible.

[0184] In addition, in explanation of the above-mentioned example, although explanation was omitted, when a removable storage device has a data processing function, it is good also as a configuration which performs mutual recognition processing between both equipments, and performs the data I/O between each equipment a condition [formation of mutual recognition] in advance of the data I/O between the data processor as a regenerative apparatus or a contents distribution terminal, and a removable storage device.

[0185] As mentioned above, it has explained in detail about this invention, referring to a specific example. However, it is obvious that this contractor can accomplish correction and substitution of this example in the range which does not deviate from the summary of this invention. That is, with the gestalt of instantiation, this invention has been indicated and it should not be interpreted restrictively. In order to judge the summary of this invention, the column of the claim indicated at the beginning should be taken into consideration.

[0186] In addition, a series of processings in which it explained into the description can be performed by the compound configuration of hardware, software, or both. When performing processing by software, it is possible to install the program which recorded the processing sequence in the memory in the computer built into the hardware of dedication, and to perform it, or to make the general purpose computer which can perform various processings install and execute a program.

[0187] For example, a program is recordable on the hard disk and ROM (Read OnlyMemory) as a record medium beforehand. Or a program is permanently [temporarily or] storable in removable record media, such as a floppy (trademark) disk, CD-ROM (Compact Disc Read Only Memory), MO (Magneto optical) disk, DVD (Digital Versatile Disc), a magnetic disk, and semiconductor memory, (record). Such a removable

record medium can be offered as the so-called software package.

[0188] In addition, a program is installed in a computer from a record medium which was mentioned above, and also it is installable in record media, such as a hard disk which carries out a wireless transfer, or transmits to a computer with a cable through networks, such as LAN (Local Area Network) and the Internet, at a computer, receives the program transmitted by making it such by computer, and is built in from a download site.

[0189] In addition, various kinds of processings indicated by the description meet the throughput or need for equipment of time series not only performing, but performing processing according to a publication, and may be performed in juxtaposition or individually. Moreover, in this description, a system is the logical set configuration of two or more equipments, and it does not restrict to what has equipment of each configuration in the same case.

[0190]

[Effect of the Invention] As mentioned above, as explained, according to the information recording device of this invention, an information regenerative apparatus and the information record approach, and the information playback approach As conditions which perform playback of the contents stored in a removable storage device like a memory card It adds to it being the device which can acquire the contents key which can be decoded by validation key block (EKB) processing. Furthermore, even if it is the case where setting out of being the same device which performed record processing to a removable storage device is attained as conditions, and two or more devices which can decode the same EKB exist A refreshable device becomes possible [limiting to the only device which stored contents in the removable storage device] about the contents stored in the removable storage device.

[0191] Furthermore, according to the information recording device of this invention, an information regenerative apparatus and the information record approach, and the information playback approach As conditions which perform playback of the contents stored in the removable storage device from the external contents distribution terminal It adds to it being the device which can acquire the contents key which can be decoded by EKB processing. Furthermore, even if it is the case where setting out of being the device same in the case of contents purchase processing as the specified device is attained as conditions, and two or more devices which can decode the same EKB exist It becomes possible to limit to the only device with which the refreshable device specified the contents stored in the removable storage device at the time of contents purchase.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing explaining the system use concept of this invention.

[Drawing 2] It is drawing showing the example of a system configuration of this invention, and the example of data utilization using a removable storage device.

[Drawing 3] They are the various keys in the system of this invention, and a tree block diagram explaining data encryption processing.

[Drawing 4] It is drawing showing the example of the various keys in the system of this invention, and the validation key block (EKB) used for distribution of data.

[Drawing 5] It is drawing showing the example of distribution which used the validation key block (EKB) of the contents key in the system of this invention, and the example of decode processing.

[Drawing 6] It is drawing showing the example of a format of the validation key block (EKB) in the system of this invention.

[Drawing 7] It is drawing explaining the configuration of the tag of the validation key block (EKB) in the system of this invention.

[Drawing 8] It is drawing showing the example of a data configuration which distributes a contents key and contents collectively with the validation key block (EKB) in the system of this invention.

[Drawing 9] It is drawing showing the example of processing in the device at the time of distributing a contents key and contents collectively with the validation key block (EKB) in the system of this invention.

[Drawing 10] It is drawing explaining the response at the time of storing the validation key block (EKB) and contents in a system of this invention in a record medium.

[Drawing 11] It is drawing explaining the example of the categorization of the hierarchy tree structure in the system of this invention.

[Drawing 12] It is drawing explaining the generation process of the simplification validation key block (EKB) in the system of this invention.

[Drawing 13] It is drawing explaining the generation process of the validation key block (EKB) in the system of this invention.

[Drawing 14] It is drawing explaining the simplification validation key block (EKB) in the system of this invention.

[Drawing 15] It is drawing showing the example of a configuration of the data

regenerative apparatus in the system of this invention.

[Drawing 16] It is drawing showing the example of data storage processing over a removable storage device in the system of this invention.

[Drawing 17] In the system of this invention, it is drawing showing the example of data stored in a removable storage device.

[Drawing 18] In the system of this invention, it is drawing showing the example of data regeneration from a removable storage device.

[Drawing 19] In the system of this invention, it is drawing showing the example of data storage processing over the removable storage device from a contents distribution terminal.

[Drawing 20] In the system of this invention, it is drawing showing the processing flow which stores contents in a removable storage device.

[Drawing 21] In the system of this invention, it is drawing showing the data storage processing flow over the removable storage device from a contents distribution terminal.

[Drawing 22] In the system of this invention, it is drawing showing the data regeneration flow from a removable storage device.

[Description of Notations]

10 Contents Distribution Means
11 Internet
12 Satellite Broadcasting Service
13 Telephone Line
14 Contents Distribution Terminal
15 Removable Storage Device
20 Data-Processing Means
21 Personal Computer (PC)
22 Portable Device (PD)
23 Cellular Phone, PDA
24 Record Regenerator, Game Terminal
25 Regenerative Apparatus
30 Storage Means
40 Contents Distribution Equipment
50 Contents Normal Purchase Terminal
51 52 Removable storage device
60 Contents Non-Normal Purchase Terminal
601 Version
602 Depth

603 Data Pointer
604 Tag Pointer
605 Signature Pointer
606 Data Division
607 Tag Section
608 Signature
100 Data Processor
110 Bus
120 I/O I/F
130 I/O I/F
131 A/D, D/A Converter
140 Cipher-Processing Means
150 ROM
160 RAM
170 CPU
180 Internal Memory
190 Storage I/F
200 Removable Storage Device
300 Contents Distribution Terminal
320 I/O I/F
330 Cipher-Processing Means
340 ROM
350 RAM
360 Control Means (CPU)
370 Storage Means
380 Storage I/F
400,500 Regenerative apparatus
600 Removable Storage Device

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－319932
（P2002－319932A）
(43)公開日　平成14年10月31日(2002.10.31)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｇ１１Ｂ　20/10	Ｈ　５Ｄ０４４
Ｇ１１Ｂ　20/10		Ｈ０４Ｌ　9/00	６０１Ｄ　５Ｊ１０４
			６０１Ａ
			６０１Ｅ

審査請求　未請求　請求項の数30　ＯＬ　（全 32 頁）

(21)出願番号　特願2001－120494(P2001－120494)

(22)出願日　平成13年４月19日(2001.4.19)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

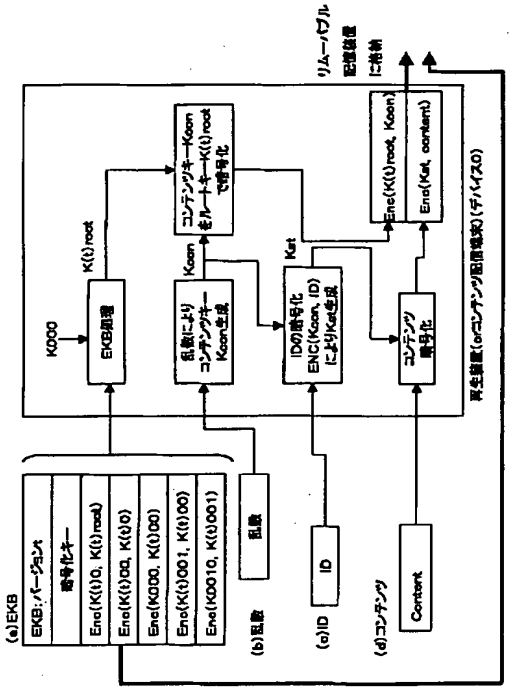
(72)発明者　岡上　拓己
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(74)代理人　100101801
弁理士　山田　英治　（外２名）

Ｆターム(参考)　5D044 AB01 AB05 AB07 GK17
5J104 AA09 AA12 AA16 EA01 EA06
EA17 EA26 LA06 NA35 NA41
PA14

(54)【発明の名称】　情報記録装置、情報再生装置、および情報記録方法、情報再生方法、並びにプログラム

(57)【要約】
【課題】　コンテンツの利用を行なうデータ処理装置を限定可能とした構成を提供する。
【解決手段】　メモリカードのようなリムーバブル記憶装置に格納したコンテンツの再生実行条件として、有効化キーブロック（ＥＫＢ）処理によって復号可能なコンテンツキーを取得可能なデバイスであること、さらに、リムーバブル記憶装置に対する記録処理を行なったデバイス、あるいはコンテンツ購入処理の際の指定デバイスであることを設定可能とした。本構成により、同一のＥＫＢを復号可能な複数のデバイスが存在する場合であっても、リムーバブル記憶装置に格納したコンテンツを再生可能なデバイスを唯一のデバイスに限定可能となる。



1

【特許請求の範囲】

【請求項１】記録媒体に情報を記録する情報記録装置において、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとからなるデバイスノードキー（ＤＮＫ）を格納した記憶手段と、

前記記録媒体に対する格納データの暗号処理を実行する暗号処理手段とを有し、

前記暗号処理手段は、

前記記録媒体の格納データの再生を行なう特定のデータ再生装置の固有値に対して暗号鍵（Ｋｃｏｎ）を適用した暗号処理を実行して、前記格納データに適用する暗号鍵（Ｋｓｔ）を生成し、該暗号鍵（Ｋｓｔ）による格納データの暗号化処理によって暗号化データ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）を生成し、前記固有値の暗号処理に適用した暗号鍵（Ｋｃｏｎ）を、前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵を用いて暗号化した暗号鍵データを生成し、

前記暗号化データと、前記暗号鍵データとを含むデータファイルと、

前記有効化キーブロック（ＥＫＢ）とを、前記記録媒体に格納する処理を実行する構成を有することを特徴とする情報記録装置。

【請求項２】前記特定のデータ再生装置は、前記情報記録装置自身であり、前記固有値は、前記情報記録装置に対応付けられた固有値であることを特徴とする請求項１に記載の情報記録装置。

【請求項３】前記情報記録装置は、

コンテンツの配信を実行するコンテンツ配信端末であり、

前記特定のデータ再生装置は、前記コンテンツ配信端末からのダウンロードコンテンツを利用するデータ再生装置であり、前記固有値は、前記データ再生装置に対応付けられた固有値であり、

前記情報記録装置は、外部から入力された前記データ再生装置に対応付けられた固有値に対して前記暗号鍵（Ｋｃｏｎ）を適用した暗号処理を実行する構成であることを特徴とする請求項１に記載の情報記録装置。

【請求項４】前記データ再生装置の固有値は、該データ再生装置に固有の電話番号、またはデータ再生装置に固有の識別データであることを特徴とする請求項１に記載の情報記録装置。

【請求項５】前記記録媒体は、前記情報記録装置に対して着脱可能なリムーバブル記録媒体であることを特徴とする請求項１に記載の情報記録装置。

【請求項６】前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、該階層ツリーの頂点ノードであるルートに対して設定されたルートキー：Ｋｒｏｏｔであることを特徴とする請求項１に記載の情報記録装置。

2

【請求項７】前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、前記デバイスノードキー（ＤＮＫ）による前記有効化キーブロック（ＥＫＢ）の復号処理により取得可能な鍵であることを特徴とする請求項１に記載の情報記録装置。

【請求項８】前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、更新可能な鍵として構成され、

前記情報記録装置は、

前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）に格納された更新された階層ツリー構成鍵を、前記デバイスノードキー（ＤＮＫ）による前記有効化キーブロック（ＥＫＢ）の復号処理により取得する構成を有することを特徴とする請求項１に記載の情報記録装置。

【請求項９】前記暗号処理手段は、

前記情報記録装置の固有値に対する暗号鍵（Ｋｃｏｎ）を乱数に基づいて生成する構成であることを特徴とする請求項１に記載の情報記録装置。

【請求項１０】記録媒体に格納された格納データの再生処理を実行する情報再生装置において、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生置固有のリーフキーとからなるデバイスノードキー（ＤＮＫ）を格納した記憶手段と、

前記記録媒体の格納データの復号処理を実行する暗号処理手段とを有し、

前記暗号処理手段は、

前記記録媒体に格納された前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）を前記デバイスノードキー（ＤＮＫ）を用いて復号して、該有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵を取得し、

前記記録媒体に格納された前記階層ツリー構成鍵を用いて暗号化した暗号鍵データの復号処理により暗号鍵（Ｋｃｏｎ）を取得し、

前記情報再生装置自身の固有値に対して、前記暗号鍵（Ｋｃｏｎ）を適用した暗号処理を実行して、前記格納データに適用する復号鍵（Ｋｓｔ）を生成し、該復号鍵（Ｋｓｔ）による格納暗号化データ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）の復号処理を実行する構成を有することを特徴とする情報再生装置。

【請求項１１】前記情報再生装置の固有値は、該情報再生装置に固有の電話番号、または情報再生装置に固有の識別データであることを特徴とする請求項１０に記載の

情報再生装置。

【請求項１２】前記記録媒体は、前記情報再生装置に対して着脱可能なリムーバブル記録媒体であることを特徴とする請求項１０に記載の情報再生装置。

【請求項１３】前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、該階層ツリーの頂点ノードであるルートに対して設定されたルートキー：Ｋｒｏｏｔであることを特徴とする請求項１０に記載の情報再生装置。

【請求項１４】前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、更新可能な鍵として構成され、

前記情報再生装置は、

前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）に格納された更新された階層ツリー構成鍵を、前記デバイスノードキー（ＤＮＫ）による前記有効化キーブロック（ＥＫＢ）の復号処理により取得する構成を有することを特徴とする請求項１０に記載の情報再生装置。

【請求項１５】複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとからなるデバイスノードキー（ＤＮＫ）を格納した記憶手段と、記録媒体に対する格納データの暗号処理を実行する暗号処理手段とを有する情報記録装置における前記記録媒体に対する情報記録方法において、

前記記録媒体の格納データの再生を行なう特定のデータ再生装置の固有値に対して暗号鍵（Ｋｃｏｎ）を適用した暗号処理を実行して、前記格納データに適用する暗号鍵（Ｋｓｔ）を生成するステップと、

前記暗号鍵（Ｋｓｔ）による格納データの暗号化処理によって暗号化データ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）を生成するステップと、

前記固有値の暗号処理に適用した暗号鍵（Ｋｃｏｎ）を、前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵を用いて暗号化した暗号鍵データを生成するステップと、

前記暗号化データと、前記暗号鍵データとを含むデータファイルと、前記有効化キーブロック（ＥＫＢ）とを、前記記録媒体に格納するステップと、

を有することを特徴とする情報記録方法。

【請求項１６】前記特定のデータ再生装置は、前記情報記録装置自身であり、前記固有値は、前記情報記録装置に対応付けられた固有値であることを特徴とする請求項１５に記載の情報記録方法。

【請求項１７】前記情報記録装置は、

コンテンツの配信を実行するコンテンツ配信端末であり、

前記特定のデータ再生装置は、前記コンテンツ配信端末からのダウンロードコンテンツを利用するデータ再生装置であり、前記固有値は、前記データ再生装置に対応付けられた固有値であり、

前記暗号鍵（Ｋｓｔ）を生成するステップは、

外部から入力された前記データ再生装置に対応付けられた固有値に対して前記暗号鍵（Ｋｃｏｎ）を適用した暗号処理を実行するステップを含むことを特徴とする請求項１５に記載の情報記録方法。

【請求項１８】前記データ再生装置の固有値は、該データ再生装置に固有の電話番号、またはデータ再生装置に固有の識別データであることを特徴とする請求項１５に記載の情報記録方法。

【請求項１９】前記記録媒体は、前記情報記録装置に対して着脱可能なリムーバブル記録媒体であることを特徴とする請求項１５に記載の情報記録方法。

【請求項２０】前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、該階層ツリーの頂点ノードであるルートに対して設定されたルートキー：Ｋｒｏｏｔであることを特徴とする請求項１５に記載の情報記録方法。

【請求項２１】前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、前記デバイスノードキー（ＤＮＫ）による前記有効化キーブロック（ＥＫＢ）の復号処理により取得可能な鍵であることを特徴とする請求項１５に記載の情報記録方法。

【請求項２２】前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、更新可能な鍵として構成され、

前記情報記録方法は、さらに、

前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）に格納された更新された階層ツリー構成鍵を、前記デバイスノードキー（ＤＮＫ）による前記有効化キーブロック（ＥＫＢ）の復号処理により取得する処理を実行するステップを含むことを特徴とする請求項１５に記載の情報記録方法。

【請求項２３】前記情報記録方法は、さらに、

前記情報記録装置の固有値に対する暗号鍵（Ｋｃｏｎ）を乱数に基づいて生成するステップを有することを特徴とする請求項１５に記載の情報記録方法。

【請求項２４】複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生置固有のリーフキーとからなるデバイスノードキー（ＤＮＫ）を格納した記憶手段と、記録媒体の格納データの復号処理を実行する暗号処理手段とを有する情報再生装置における、前記記録媒体に格納された格納データの再生処理を実行する情報再生方法において、

前記記録媒体に格納された前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）を前記デバイスノードキー（ＤＮＫ）を用いて復号して、該有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵を取得するステップと、

前記記録媒体に格納された前記階層ツリー構成鍵を用いて暗号化した暗号鍵データの復号処理により暗号鍵（Ｋｃｏｎ）を取得するステップと、

前記情報再生装置自身の固有値に対して、前記暗号鍵（Ｋｃｏｎ）を適用した暗号処理を実行して、前記格納データに適用する復号鍵（Ｋｓｔ）を生成し、該復号鍵（Ｋｓｔ）による格納暗号化データ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）の復号処理を実行するステップと、

を有することを特徴とする情報再生方法。

【請求項２５】前記情報再生装置の固有値は、該情報再生装置に固有の電話番号、または情報再生装置に固有の識別データであることを特徴とする請求項２４に記載の情報再生方法。

【請求項２６】前記記録媒体は、前記情報再生装置に対して着脱可能なリムーバブル記録媒体であることを特徴とする請求項２４に記載の情報再生方法。

【請求項２７】前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、該階層ツリーの頂点ノードであるルートに対して設定されたルートキー：Ｋｒｏｏｔであることを特徴とする請求項２４に記載の情報再生方法。

【請求項２８】前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、更新可能な鍵として構成され、

前記情報再生方法は、さらに、

前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）に格納された更新された階層ツリー構成鍵を、前記デバイスノードキー（ＤＮＫ）による前記有効化キーブロック（ＥＫＢ）の復号処理により取得するステップを含むことを特徴とする請求項２４に記載の情報再生方法。

【請求項２９】複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとからなるデバイスノードキー（ＤＮＫ）を格納した記憶手段と、記録媒体に対する格納データの暗号処理を実行する暗号処理手段とを有する情報記録装置における前記記録媒体に対する情報記録処理をコンピュータ・システム上で実行せしめるプログラムであって、前記プログラムは、

前記記録媒体の格納データの再生を行なう特定のデータ再生装置の固有値に対して暗号鍵（Ｋｃｏｎ）を適用した暗号処理を実行して、前記格納データに適用する暗号鍵（Ｋｓｔ）を生成するステップと、

前記暗号鍵（Ｋｓｔ）による格納データの暗号化処理によって暗号化データ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）を生成するステップと、

前記固有値の暗号処理に適用した暗号鍵（Ｋｃｏｎ）を、前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵を用いて暗号化した暗号鍵データを生成するステップと、

前記暗号化データと、前記暗号鍵データとを含むデータファイルと、前記有効化キーブロック（ＥＫＢ）とを、前記記録媒体に格納するステップと、

を有することを特徴とするプログラム。

【請求項３０】複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生置固有のリーフキーとからなるデバイスノードキー（ＤＮＫ）を格納した記憶手段と、記録媒体の格納データの復号処理を実行する暗号処理手段とを有する情報再生装置における、前記記録媒体に格納された格納データの再生処理をコンピュータ・システム上で実行せしめるプログラムであって、前記プログラムは、

前記記録媒体に格納された前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）を前記デバイスノードキー（ＤＮＫ）を用いて復号して、該有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵を取得するステップと、

前記記録媒体に格納された前記階層ツリー構成鍵を用いて暗号化した暗号鍵データの復号処理により暗号鍵（Ｋｃｏｎ）を取得するステップと、

前記情報再生装置自身の固有値に対して、前記暗号鍵（Ｋｃｏｎ）を適用した暗号処理を実行して、前記格納データに適用する復号鍵（Ｋｓｔ）を生成し、該復号鍵（Ｋｓｔ）による格納暗号化データ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）の復号処理を実行するステップと、

を有することを特徴とするプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報記録装置、情報再生装置、および情報記録方法、情報再生方法、並びにプログラムに関する。特に、音楽、画像、ゲーム、プログラム等様々なコンテンツの再生を、正当なコンテンツ利用機器においてのみ実行可能とし、リムーバブル記憶装置を介した不正なコンテンツの移動再生を排除する構成を実現した情報記録装置、情報再生装置、および情報記録方法、情報再生方法、並びにプログラムに関する。

【０００２】

【従来の技術】昨今、音楽データ、ゲームプログラム、画像データ等、様々なソフトウエアデータ（以下、これ

らをコンテンツ（Content）と呼ぶ）を、インターネット等のネットワーク、あるいは、メモリカード、ＤＶＤ、ＣＤ等の流通可能な記憶媒体を介して流通させるコンテンツ流通が盛んになってきている。これらの流通コンテンツは、ユーザの所有するＰＣ（Personal Computer）、携帯電話、データ再生装置、あるいはゲーム機器などによって直接データを受信して内部メモリに格納したり、あるいはメモリカード、ＣＤ、ＤＶＤ等の記憶媒体を介してデータを内部メモリに格納するなどの方法により、コンテンツの購入、再生処理が実行される。

【０００３】携帯電話、データ再生装置、ゲーム機器、ＰＣ等の情報機器には、流通コンテンツをネットワークから受信するための受信機能、あるいはＤＶＤ、ＣＤ等にアクセスするためのインタフェースを有し、さらにコンテンツの再生に必要となる制御手段、プログラム、データのメモリ領域として使用されるＲＡＭ、ＲＯＭ等を有する。

【０００４】音楽データ、画像データ、あるいはプログラム等の様々なコンテンツは、再生機器として利用される携帯電話、データ再生装置、ゲーム機器、ＰＣ等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により、例えば内蔵、あるいは着脱自在の記憶媒体から呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

【０００５】ゲームプログラム、音楽データ、画像データ等、多くのソフトウエア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウエアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

【０００６】ユーザに対する利用制限を実現する１つの手法が、配布コンテンツの暗号化処理である。すなわち、例えばインターネット等を介して暗号化された音声データ、画像データ、ゲームプログラム等の各種コンテンツを配布するとともに、正規ユーザであると確認された者に対してのみ、配布された暗号化コンテンツを復号する手段、すなわち復号鍵を付与する構成である。

【０００７】暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

【０００８】暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類あるが、その１つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にＤＥＳ（データ暗号標準：Deta encryption standard）がある。

【０００９】上述の暗号化処理、復号化に用いられる暗号化鍵、復号化鍵は、例えばあるパスワード等に基づいてハッシュ関数等の一方向性関数を適用して得ることができる。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めることは実質上不可能となる。

【００１０】また、暗号化するときに使用する暗号化鍵による処理と、復号するときに使用する復号化鍵の処理とを異なるアルゴリズムとした方式がいわゆる公開鍵暗号化方式と呼ばれる方式である。公開鍵暗号化方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が発行した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号処理が可能となる。秘密鍵は、公開鍵を発行した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号化方式の代表的なものにはＲＳＡ（Rivest-Shamir-Adleman）暗号がある。このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。

【００１１】

【発明が解決しようとする課題】しかしながら、一旦、正規購入者によって購入されたコンテンツが復号され、例えばメモリカードなどのリムーバブル記憶装置にそのままコピーされると、コンテンツ格納記憶装置をコンテンツの非購入者である他のユーザの持つ機器にセットして再生されたり、さらに他の記憶装置にコピーされて、さらに多くのユーザに利用されるなどの可能性がある。このように、1回のコンテンツの正規購入に基づいて、無秩序なコンテンツの２次流通が発生する可能性がある。

【００１２】本発明は、このような従来技術の問題点を解決するものであり、メモリカード等のリムーバブル記憶装置に格納されたコンテンツをコンテンツの正規購入者の機器においてのみ利用可能とし、メモリカード等に格納されたコンテンツを他の機器において不正に再生、利用されることを防止することを目的とする。

【００１３】さらに、本発明は、例えばサービスプロバイダの管理するコンテンツ配信端末に、ユーザの所有す

るメモリカード等のリムーバブル記憶装置をセットしてコンテンツを記憶装置に格納してコンテンツの購入を実行する場合においても、購入コンテンツを正規購入ユーザの持つ特定の再生機器においてのみ利用可能とする構成を提供することを目的とする。

【００１４】

【課題を解決するための手段】本発明の第１の側面は、記録媒体に情報を記録する情報記録装置において、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとからなるデバイスノードキー（ＤＮＫ）を格納した記憶手段と、前記記録媒体に対する格納データの暗号処理を実行する暗号処理手段とを有し、前記暗号処理手段は、前記記録媒体の格納データの再生を行なう特定のデータ再生装置の固有値に対して暗号鍵（Ｋｃｏｎ）を適用した暗号処理を実行して、前記格納データに適用する暗号鍵（Ｋｓｔ）を生成し、該暗号鍵（Ｋｓｔ）による格納データの暗号化処理によって暗号化データ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）を生成し、前記固有値の暗号処理に適用した暗号鍵（Ｋｃｏｎ）を、前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵を用いて暗号化した暗号鍵データを生成し、前記暗号化データと、前記暗号鍵データとを含むデータファイルと、前記有効化キーブロック（ＥＫＢ）とを、前記記録媒体に格納する処理を実行する構成を有することを特徴とする情報記録装置にある。

【００１５】さらに、本発明の情報記録装置の一実施態様において、前記特定のデータ再生装置は、前記情報記録装置自身であり、前記固有値は、前記情報記録装置に対応付けられた固有値であることを特徴とする。

【００１６】さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、コンテンツの配信を実行するコンテンツ配信端末であり、前記特定のデータ再生装置は、前記コンテンツ配信端末からのダウンロードコンテンツを利用するデータ再生装置であり、前記固有値は、前記データ再生装置に対応付けられた固有値であり、前記情報記録装置は、外部から入力された前記データ再生装置に対応付けられた固有値に対して前記暗号鍵（Ｋｃｏｎ）を適用した暗号処理を実行する構成であることを特徴とする。

【００１７】さらに、本発明の情報記録装置の一実施態様において、前記データ再生装置の固有値は、該データ再生装置に固有の電話番号、またはデータ再生装置に固有の識別データであることを特徴とする。

【００１８】さらに、本発明の情報記録装置の一実施態様において、前記記録媒体は、前記情報記録装置に対して着脱可能なリムーバブル記録媒体であることを特徴とする。

【００１９】さらに、本発明の情報記録装置の一実施態様において、前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、該階層ツリーの頂点ノードであるルートに対して設定されたルートキー：Ｋｒｏｏｔであることを特徴とする。

【００２０】さらに、本発明の情報記録装置の一実施態様において、前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、前記デバイスノードキー（ＤＮＫ）による前記有効化キーブロック（ＥＫＢ）の復号処理により取得可能な鍵であることを特徴とする。

【００２１】さらに、本発明の情報記録装置の一実施態様において、前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、更新可能な鍵として構成され、前記情報記録装置は、前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）に格納された更新された階層ツリー構成鍵を、前記デバイスノードキー（ＤＮＫ）による前記有効化キーブロック（ＥＫＢ）の復号処理により取得する構成を有することを特徴とする。

【００２２】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記情報記録装置の固有値に対する暗号鍵（Ｋｃｏｎ）を乱数に基づいて生成する構成であることを特徴とする。

【００２３】さらに、本発明の第２の側面は、記録媒体に格納された格納データの再生処理を実行する情報再生装置において、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生置固有のリーフキーとからなるデバイスノードキー（ＤＮＫ）を格納した記憶手段と、前記記録媒体の格納データの復号処理を実行する暗号処理手段とを有し、前記暗号処理手段は、前記記録媒体に格納された前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）を前記デバイスノードキー（ＤＮＫ）を用いて復号して、該有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵を取得し、前記記録媒体に格納された前記階層ツリー構成鍵を用いて暗号化した暗号鍵データの復号処理により暗号鍵（Ｋｃｏｎ）を取得し、前記情報再生装置自身の固有値に対して、前記暗号鍵（Ｋｃｏｎ）を適用した暗号処理を実行して、前記格納データに適用する復号鍵（Ｋｓｔ）を生成し、該復号鍵（Ｋｓｔ）による格納暗号化データ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）の復号処理を実行する構成を有することを特徴とする情報再生装置にある。

【００２４】さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置の固有値は、該情報再生装置に固有の電話番号、または情報再生装置に固有の識別データであることを特徴とする。

【００２５】さらに、本発明の情報再生装置の一実施態様において、前記記録媒体は、前記情報再生装置に対して着脱可能なリムーバブル記録媒体であることを特徴とする。

【００２６】さらに、本発明の情報再生装置の一実施態様において、前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、該階層ツリーの頂点ノードであるルートに対して設定されたルートキー：Ｋｒｏｏｔであることを特徴とする。

【００２７】さらに、本発明の情報再生装置の一実施態様において、前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、更新可能な鍵として構成され、前記情報再生装置は、前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）に格納された更新された階層ツリー構成鍵を、前記デバイスノードキー（ＤＮＫ）による前記有効化キーブロック（ＥＫＢ）の復号処理により取得する構成を有することを特徴とする。

【００２８】さらに、本発明の第３の側面は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとからなるデバイスノードキー（ＤＮＫ）を格納した記憶手段と、記録媒体に対する格納データの暗号処理を実行する暗号処理手段とを有する情報記録装置における前記記録媒体に対する情報記録方法において、前記記録媒体の格納データの再生を行なう特定のデータ再生装置の固有値に対して暗号鍵（Ｋｃｏｎ）を適用した暗号処理を実行して、前記格納データに適用する暗号鍵（Ｋｓｔ）を生成するステップと、前記暗号鍵（Ｋｓｔ）による格納データの暗号化処理によって暗号化データ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）を生成するステップと、前記固有値の暗号処理に適用した暗号鍵（Ｋｃｏｎ）を、前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵を用いて暗号化した暗号鍵データを生成するステップと、前記暗号化データと、前記暗号鍵データとを含むデータファイルと、前記有効化キーブロック（ＥＫＢ）とを、前記記録媒体に格納するステップと、を有することを特徴とする情報記録方法にある。

【００２９】さらに、本発明の情報記録方法の一実施態様において、前記特定のデータ再生装置は、前記情報記録装置自身であり、前記固有値は、前記情報記録装置に対応付けられた固有値であることを特徴とする。

【００３０】さらに、本発明の情報記録方法の一実施態様において、前記情報記録装置は、コンテンツの配信を実行するコンテンツ配信端末であり、前記特定のデータ再生装置は、前記コンテンツ配信端末からのダウンロードコンテンツを利用するデータ再生装置であり、前記固有値は、前記データ再生装置に対応付けられた固有値であり、前記暗号鍵（Ｋｓｔ）を生成するステップは、外部から入力された前記データ再生装置に対応付けられた固有値に対して前記暗号鍵（Ｋｃｏｎ）を適用した暗号処理を実行するステップを含むことを特徴とする。

【００３１】さらに、本発明の情報記録方法の一実施態様において、前記データ再生装置の固有値は、該データ再生装置に固有の電話番号、またはデータ再生装置に固有の識別データであることを特徴とする。

【００３２】さらに、本発明の情報記録方法の一実施態様において、前記記録媒体は、前記情報記録装置に対して着脱可能なリムーバブル記録媒体であることを特徴とする。

【００３３】さらに、本発明の情報記録方法の一実施態様において、前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、該階層ツリーの頂点ノードであるルートに対して設定されたルートキー：Ｋｒｏｏｔであることを特徴とする。

【００３４】さらに、本発明の情報記録方法の一実施態様において、前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、前記デバイスノードキー（ＤＮＫ）による前記有効化キーブロック（ＥＫＢ）の復号処理により取得可能な鍵であることを特徴とする。

【００３５】さらに、本発明の情報記録方法の一実施態様において、前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、更新可能な鍵として構成され、前記情報記録方法は、さらに、前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）に格納された更新された階層ツリー構成鍵を、前記デバイスノードキー（ＤＮＫ）による前記有効化キーブロック（ＥＫＢ）の復号処理により取得する処理を実行するステップを含むことを特徴とする。

【００３６】さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法は、さらに、前記情報記録装置の固有値に対する暗号鍵（Ｋｃｏｎ）を乱数に基づいて生成するステップを有することを特徴とする。

【００３７】さらに、本発明の第４の側面は、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生置固有のリーフキーとからなるデバイスノードキー（ＤＮＫ）を格納した記憶手段と、記録媒体の格納データの復号処理を実行する暗号処理手段とを有する情報再生装置における、前記記録媒体に格納された格納データの再生処理を実行する情報再生方法において、前記記録媒体に格納された前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）を前記デバイスノードキー（ＤＮＫ）を用いて復号して、該有効化

キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵を取得するステップと、前記記録媒体に格納された前記階層ツリー構成鍵を用いて暗号化した暗号鍵データの復号処理により暗号鍵（Ｋｃｏｎ）を取得するステップと、前記情報再生装置自身の固有値に対して、前記暗号鍵（Ｋｃｏｎ）を適用した暗号処理を実行して、前記格納データに適用する復号鍵（Ｋｓｔ）を生成し、該復号鍵（Ｋｓｔ）による格納暗号化データ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）の復号処理を実行するステップと、を有することを特徴とする情報再生方法にある。

【００３８】さらに、本発明の情報再生方法の一実施態様において、前記情報再生装置の固有値は、該情報再生装置に固有の電話番号、または情報再生装置に固有の識別データであることを特徴とする。

【００３９】さらに、本発明の情報再生方法の一実施態様において、前記記録媒体は、前記情報再生装置に対して着脱可能なリムーバブル記録媒体であることを特徴とする。

【００４０】さらに、本発明の情報再生方法の一実施態様において、前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、該階層ツリーの頂点ノードであるルートに対して設定されたルートキー：Ｋｒｏｏｔであることを特徴とする。

【００４１】さらに、本発明の情報再生方法の一実施態様において、前記有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵は、更新可能な鍵として構成され、前記情報再生方法は、さらに、前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）に格納された更新された階層ツリー構成鍵を、前記デバイスノードキー（ＤＮＫ）による前記有効化キーブロック（ＥＫＢ）の復号処理により取得するステップを含むことを特徴とする。

【００４２】さらに、本発明の第５の側面は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとからなるデバイスノードキー（ＤＮＫ）を格納した記憶手段と、記録媒体に対する格納データの暗号処理を実行する暗号処理手段とを有する情報記録装置における前記記録媒体に対する情報記録処理をコンピュータ・システム上で実行せしめるプログラムであって、前記プログラムは、前記記録媒体の格納データの再生を行なう特定のデータ再生装置の固有値に対して暗号鍵（Ｋｃｏｎ）を適用した暗号処理を実行して、前記格納データに適用する暗号鍵（Ｋｓｔ）を生成するステップと、前記暗号鍵（Ｋｓｔ）による格納データの暗号化処理によって暗号化データ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）を生成するステップと、前記固有値の暗号処理に適用した暗号鍵（Ｋｃｏｎ）を、前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵を用いて暗号化した暗号鍵データを生成するステップと、前記暗号化データと、前記暗号鍵データとを含むデータファイルと、前記有効化キーブロック（ＥＫＢ）とを、前記記録媒体に格納するステップと、を有することを特徴とするプログラムにある。

【００４３】さらに、本発明の第６の側面は、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生置固有のリーフキーとからなるデバイスノードキー（ＤＮＫ）を格納した記憶手段と、記録媒体の格納データの復号処理を実行する暗号処理手段とを有する情報再生装置における、前記記録媒体に格納された格納データの再生処理をコンピュータ・システム上で実行せしめるプログラムであって、前記プログラムは、前記記録媒体に格納された前記階層ツリーの上位キーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）を前記デバイスノードキー（ＤＮＫ）を用いて復号して、該有効化キーブロック（ＥＫＢ）に格納された階層ツリー構成鍵を取得するステップと、前記記録媒体に格納された前記階層ツリー構成鍵を用いて暗号化した暗号鍵データの復号処理により暗号鍵（Ｋｃｏｎ）を取得するステップと、前記情報再生装置自身の固有値に対して、前記暗号鍵（Ｋｃｏｎ）を適用した暗号処理を実行して、前記格納データに適用する復号鍵（Ｋｓｔ）を生成し、該復号鍵（Ｋｓｔ）による格納暗号化データ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）の復号処理を実行するステップと、を有することを特徴とするプログラムにある。

【００４４】なお、本発明のプログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する媒体、例えば、ＣＤやＦＤ、ＭＯなどの記憶媒体に格納されて提供可能であり、またネットワークなどの伝送媒体などによっても提供可能なプログラムである。

【００４５】このようなプログラムは、プロセッサ制御の下でプログラムの読み取りに基づき、システムの有する各種機能の実行を規程するとともに、システム上の協働的作用を発揮するものであり、本発明の他の側面と同様の作用効果を得ることができるものである。

【００４６】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本発明においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【００４７】

【発明の実施の形態】［システム概要］図１に本発明のデータ処理システムの適用可能なコンテンツ配信システ

ム例を示す。コンテンツ配信手段１０は、データ処理手段２０に対して、音楽、画像、ゲーム、プログラム等様々なコンテンツを暗号化データあるいは平文（非暗号化）データとして送信する。データ処理手段２０では、受信したコンテンツを必要に応じて復号して、画像データ、音声データの再生、あるいは各種プログラムを実行し、また内部メモリ、リムーバブルメモリに格納するなどの処理を実行する。コンテンツの配信手段１０とデータ処理手段２０との間のデータ交換は、電話回線、インターネット等のネットワークを介して、あるいはメモリカード、ＤＶＤ、ＣＤ、その他の記憶媒体を介して実行される。

【００４８】コンテンツ配信手段１０としては、インターネット１１、衛星放送１２、電話回線１３、サービスプロバイダ等が駅あるいは店舗等に設置したコンテンツ配信端末１４等があり、コンテンツ配信端末１４からのコンテンツ購入の際には、メモリカードなどのリムーバブル記憶装置１５をコンテンツ配信端末１４にセットしてコンテンツを格納する。なお、本発明のシステムでは、このデータ移動の際に後段で詳細説明する暗号化処理を含む処理が実行される。

【００４９】データ処理手段２０のデバイスとしては、パーソナルコンピュータ（ＰＣ）２１、ポータブルデバイス（ＰＤ）２２、携帯電話、ＰＤＡ（Personal Digital Assistants）等の携帯機器２３、ＤＶＤ、ＣＤプレーヤ等の記録再生器、ゲーム端末２４、記録再生装置２５等がある。これらデータ処理手段２０の各デバイスは、コンテンツ配信手段１０から提供されるコンテンツをネットワーク等の通信手段あるいは、他のデータ処理手段、または、データ記憶手段３０から取得可能である。

【００５０】データ記憶手段３０には、フラッシュメモリ等の記憶手段を備えたＤＶＤ，ＣＤ、また、暗号処理機能を有する記憶手段としてのメモリカード（具体例としてはメモリスティック(Memory Stick:商標)）なども含まれる。

【００５１】データ処理手段２０の各々は、購入したコンテンツデータを内部メモリ、あるいはメモリカード等のリムーバブル記憶手段に格納することができる。

【００５２】本発明のシステムにおいては、コンテンツをデータ処理手段２０の内部メモリからリムーバブル記憶手段３０に出力して格納する際、および、コンテンツ購入時にコンテンツ配信端末１４の内部メモリに格納されたコンテンツをリムーバブル記憶装置に格納する際に、後段で詳細に説明するコンテンツの暗号化処理を含む処理が実行され、正当な購入者の機器においてのみ再生可能とする処理がなされる。

【００５３】図２に、代表的なコンテンツデータの移動処理例を示す。図２に示すシステムは、コンテンツ正規購入端末５０と、コンテンツの正規購入を実行していないコンテンツ非正規購入端末６０を示し、コンテンツ正規購入端末５０によって購入されたコンテンツが例えばフラッシュメモリなど書き換え可能な半導体メモリを内蔵したメモリカード（例えばメモリスティック(Memory Stick:商標)）等のリムーバブル記憶装置５２を介してコンテンツ非正規購入端末６０によって利用される可能性を説明する図である。

【００５４】コンテンツ正規購入端末５０は、インターネット等のネットワーク、電話回線を介して、あるいはコンテンツ配信端末４０にリムーバブル記憶装置５１をセットしてオーディオデータ、画像データ、プログラム等のコンテンツを格納するなどの処理を通じてコンテンツの購入を行なうことができる。これらのコンテンツは対価を支払ったユーザに提供される有料コンテンツであったり、特定の登録ユーザ向けに提供されるコンテンツが含まれる。コンテンツ正規購入端末５０は、は、コンテンツデータを格納するに当たって、必要に応じて、サービスプロバイダのホストコンピュータとの間で認証処理および課金処理などを行う。

【００５５】コンテンツ正規購入端末５０は、正規な手続きにより購入したコンテンツを内部メモリに格納して再生する処理が可能である。また、購入コンテンツをリムーバブル記憶装置５２に格納する処理も可能であり、これをコンテンツ非正規購入端末６０にセットすることが可能である。また、コンテンツ正規購入端末５０がコンテンツ配信端末４０にセットしてコンテンツの購入を行なったリムーバブル記憶装置５１を直接コンテンツ非正規購入端末６０にセットすることも可能である。

【００５６】本発明のシステムにおいては、これらのコンテンツ非正規購入端末６０にセットされたリムーバブル記憶装置５２、またはリムーバブル記憶装置５１からのコンテンツ再生を排除し、コンテンツ正規購入端末５０においてのみ再生可能とする処理がなされる。

【００５７】図２に示すリムーバブル記憶装置５１、５２に対するコンテンツ正規購入端末５０または、コンテンツ配信端末からのコンテンツデータの格納の際にはコンテンツの暗号化処理が実行され、暗号化コンテンツの復号処理をコンテンツ正規購入端末５０においてのみ可能とする処理がなされる。以下、これらの処理の詳細について説明する。

【００５８】［キー配信構成としてのツリー（木）構造について］上述のようなコンテンツに対する暗号処理に適用する暗号鍵、例えばコンテンツの暗号処理に適用するコンテンツキー、またはコンテンツキーを暗号化するためのコンテンツキー暗号化キー等の様々な暗号処理キーを、安全に正当なライセンスを持つデバイスに配信する構成を提供する階層ツリー構成について図３以下を用いて説明する。

【００５９】図３の最下段に示すナンバ０～１５がコンテンツデータの再生、実行を行なうデータ処理手段２０

を構成する個々のデバイス、例えばコンテンツ（音楽データ）再生装置である。すなわち図３に示す階層ツリー（木）構造の各葉(リーフ：leaf)がそれぞれのデバイスに相当する。

【００６０】各デバイス０～１５は、製造時あるいは出荷時、あるいはその後において、図３に示す階層ツリー（木）構造における、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーからなるキーセットをメモリに格納する。これらキーセットをデバイスノードキー（ＤＮＫ）と呼ぶ。図３の最下段に示すＫ０００００～Ｋ１１１１が各デバイス０～１５にそれぞれ割り当てられたリーフキーであり、最上段のＫｒｏｏｔ（ルートキー）から、最下段から２番目の節（ノード）に記載されたキー：Ｋｒｏｏｔ～Ｋ１１１をノードキーとする。

【００６１】図３に示すツリー構成において、例えばデバイス０はリーフキーＫ００００と、ノードキー：Ｋ０００、Ｋ００、Ｋ０、Ｋｒｏｏｔをデバイスノードキー（ＤＮＫ）として所有する。デバイス５はＫ０１０１、Ｋ０１０、Ｋ０１、Ｋ０、Ｋｒｏｏｔをデバイスノードキー（ＤＮＫ）として所有する。デバイス１５は、Ｋ１１１１、Ｋ１１１、Ｋ１１、Ｋ１、Ｋｒｏｏｔをデバイスノードキー（ＤＮＫ）として所有する。なお、図３のツリーにはデバイスが０～１５の１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【００６２】また、図３のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたフラッシュメモリ等を使用したメモリカード、ＤＶＤ、ＣＤ、ＭＤ等、様々なタイプの記憶装置を利用可能なデバイスが含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図３に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

【００６３】これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図３の点線で囲んだ部分、すなわちデバイス０，１，２，３を同一の記録媒体を用いる１つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、各デバイス共通に使用するコンテンツキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図３の点線で囲んだ部分、すなわちデバイス０，１，２，３を１つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図３のツリー中に複数存在する。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、メッセージデータ配信手段として機能する。

【００６４】なお、ノードキー、リーフキーは、ある１つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【００６５】このツリー構造において、図３から明らかなように、１つのグループに含まれる３つのデバイス０，１，２，３はノードキーとして共通のキーＫ００、Ｋ０、Ｋｒｏｏｔを保有する。このノードキー共有構成を利用することにより、例えば共通のコンテンツキーをデバイス０，１，２，３のみに提供することが可能となる。たとえば、共通に保有するノードキーＫ００自体をコンテンツキーとして設定すれば、新たな鍵送付を実行することなくデバイス０，１，２，３のみに共通のコンテンツキーの設定が可能である。また、新たなコンテンツキーＫｃｏｎをノードキーＫ００で暗号化した値Ｅｎｃ（Ｋ００，Ｋｃｏｎ）を、ネットワークを介してあるいは記録媒体に格納してデバイス０，１，２，３に配布すれば、デバイス０，１，２，３のみが、それぞれのデバイスにおいて保有する共有ノードキーＫ００を用いて暗号Ｅｎｃ（Ｋ００，Ｋｃｏｎ）を解いてコンテンツキー：Ｋｃｏｎを得ることが可能となる。なお、Ｅｎｃ（Ｋａ，Ｋｂ）はＫｂをＫａによって暗号化したデータであることを示す。

【００６６】また、ある時点ｔにおいて、デバイス３の所有する鍵：Ｋ００１１,Ｋ００１,Ｋ００,Ｋ０,Ｋｒｏｏｔが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキー：Ｋ００１,Ｋ００,Ｋ０,Ｋｒｏｏｔをそれぞれ新たな鍵Ｋ（ｔ）００１,Ｋ（ｔ）００,Ｋ（ｔ）０,Ｋ（ｔ）ｒｏｏｔに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）：ｔの更新キーであることを示す。

【００６７】更新キーの配布処理について説明する。キーの更新は、例えば、図４（Ａ）に示す有効化キーブロック（ＥＫＢ：Enabling Key Block）と呼ばれるブロックデータをネットワークを介して、あるいは記録媒体に格納して各デバイスに供給することによって実行され

る。有効化キーブロック（ＥＫＢ）は、更新キーを暗号化したデータによって構成される。有効化キーブロック（ＥＫＢ）は、キー更新ブロック（ＫＲＢ：Key Renewal Block）と呼ばれることもある。

【００６８】図４に示す有効化キーブロック（ＥＫＢ）は、ノードキーの更新の必要なデバイスにおいてのみ処理可能、すなわち、自己のデバイスノードキー（ＤＮＫ）を用いて復号可能なデータ構成を持つＥＫＢである。図４の例は、図３に示すツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布することを目的として形成されたブロックデータであり、デバイス０，１，２の有する各デバイスノードキー（ＤＮＫ）を用いて復号可能なデータ構成を持つ。デバイス０，デバイス１は、有効化キーブロック（ＥＫＢ）の復号処理により、更新ノードキーとしてＫ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）ｒｏｏｔが取得され、デバイス２は、更新ノードキーとしてＫ（ｔ）００１、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）ｒｏｏｔが取得される。

【００６９】例えば、図４（Ａ）のＥＫＢに示されるようにＥＫＢには複数の暗号化キーが含まれる。最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自身の持つリーフキーによってこの暗号化キーを復号し、Ｋ（ｔ）００１を得ることができる。また、復号により得たＫ（ｔ）００１を用いて、図４（Ａ）の下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）を復号可能となり、更新ノードキーＫ（ｔ）００を得ることができる。以下順次、図４（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図４（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）ｒｏｏｔ）を復号しＫ（ｔ）ｒｏｏｔを得る。一方、デバイスＫ０００．Ｋ０００１は、ノードキーＫ０００は更新する対象に含まれておらず、更新ノードキーとして必要なのは、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）ｒｏｏｔである。デバイスＫ０００．Ｋ０００１は、図４（Ａ）の上から３段目の暗号化キーＥｎｃ（Ｋ０００，Ｋ（ｔ）００）を復号しＫ（ｔ）００、を取得し、以下、図４（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図４（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）ｒｏｏｔ）を復号しＫ（ｔ）ｒｏｏｔを得る。このようにして、デバイス０，１，２は更新した鍵Ｋ（ｔ）００１，Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）ｒｏｏｔを得ることができる。なお、図４（Ａ）のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【００７０】図３に示すツリー構造の上位段のノードキー：Ｋ（ｔ）０，Ｋ（ｔ）ｒｏｏｔの更新が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図４（Ｂ）の有効化キーブロック（ＥＫＢ）を用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

【００７１】図４（Ｂ）に示すＥＫＢは、例えば特定のグループにおいて共有する新たなコンテンツキーを配布する場合に利用可能である。具体例として、図３に点線で示すグループ内のデバイス０，１，２，３がある記録媒体を用いており、新たな共通のコンテンツキーＫ（ｔ）ｃｏｎが必要であるとする。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００を用いて新たな共通の更新コンテンツキー：Ｋ（ｔ）ｃｏｎを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｃｏｎ）を図４（Ｂ）に示すＥＫＢとともに配布する。この配布により、デバイス４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

【００７２】すなわち、デバイス０，１，２はＥＫＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号すれば、ｔ時点でのコンテンツキーＫ（ｔ）ｃｏｎを得ることが可能になる。

【００７３】［ＥＫＢを使用したコンテンツキーの配布］図５に、ｔ時点でのコンテンツキーＫ（ｔ）ｃｏｎを得る処理例として、Ｋ（ｔ）００を用いて新たな共通のコンテンツキーＫ（ｔ）ｃｏｎを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｃｏｎ）と図４（Ｂ）に示すＥＫＢとを記録媒体を介して受領したデバイス０の処理を示す。すなわちＥＫＢによる暗号化メッセージデータをコンテンツキーＫ（ｔ）ｃｏｎとした例である。

【００７４】図５に示すように、デバイス０は、記録媒体に格納されている世代：ｔ時点のＥＫＢと自分があらかじめ格納しているノードキーＫ０００を用いて上述したと同様のＥＫＢ処理により、ノードキーＫ（ｔ）００を生成する。さらに、復号した更新ノードキーＫ（ｔ）００を用いて更新コンテンツキーＫ（ｔ）ｃｏｎを復号して、後にそれを使用するために自分だけが持つリーフキーＫ０００００で暗号化して格納する。

【００７５】［ＥＫＢのフォーマット］図６に有効化キーブロック（ＥＫＢ）のフォーマット例を示す。バージョン６０１は、有効化キーブロック（ＥＫＢ）のバージョンを示す識別子である。なお、バージョンは最新のＥＫＢを識別する機能とコンテンツとの対応関係を示す機能を持つ。デプスは、有効化キーブロック（ＥＫＢ）の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ６０３は、有効化キーブロック（ＥＫＢ）中のデータ部の位置を示すポインタであり、タグポインタ６０４はタグ部の位置、署名ポインタ６０５は署名の位置を示すポインタである。

【００７６】データ部６０６は、例えば更新するノード

キーを暗号化したデータを格納する。例えば図５に示すような更新されたノードキーに関する各暗号化キー等を格納する。

【００７７】タグ部６０７は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図７を用いて説明する。図７では、データとして先に図４（Ａ）で説明した有効化キーブロック（ＥＫＢ）を送付する例を示している。この時のデータは、図７の表（ｂ）に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キーＫ（ｔ）ｒｏｏｔが含まれているので、トップノードアドレスはＫｒｏｏｔとなる。このとき、例えば最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）ｒｏｏｔ）は、図７の（ａ）に示す階層ツリーに示す位置にある。ここで、次のデータは、Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが０、ない場合は１が設定される。タグは｛左（Ｌ）タグ，右（Ｒ）タグ｝として設定される。最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）ｒｏｏｔ）の左にはデータがあるので、Ｌタグ＝０、右にはデータがないので、Ｒタグ＝１となる。以下、すべてのデータにタグが設定され、図７（ｃ）に示すデータ列、およびタグ列が構成される。

【００７８】タグは、データＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）がツリー構造のどこに位置しているのかを示すために設定されるものである。データ部に格納されるキーデータＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）．．．は、単純に暗号化されたキーの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化キーのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図４で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、

０：Ｅｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）ｒｏｏｔ）
００：Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）
０００：Ｅｎｃ（Ｋ（（ｔ）０００，Ｋ（Ｔ）００）
．．．

のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

【００７９】図６に戻って、ＥＫＢフォーマットについてさらに説明する。署名（Signature）は、有効化キーブロック（ＥＫＢ）を発行した例えば鍵管理センタ、コンテンツロバイダ、決済機関等が実行する電子署名である。ＥＫＢを受領したデバイスは署名検証によって正当な有効化キーブロック（ＥＫＢ）発行者が発行した有効化キーブロック（ＥＫＢ）であることを確認する。

【００８０】［ＥＫＢを使用したコンテンツキーおよびコンテンツの配信］上述の例では、コンテンツキーのみをＥＫＢとともに送付する例について説明したが、コンテンツキーで暗号化したコンテンツと、コンテンツキー暗号キーで暗号化したコンテンツキーと、ＥＫＢによって暗号化したコンテンツキー暗号キーを併せて送付する構成について以下説明する。

【００８１】図８にこのデータ構成を示す。図８（ａ）に示す構成において、Ｅｎｃ（Ｋｃｏｎ，ｃｏｎｔｅｎｔ）８０１は、コンテンツ（Content）をコンテンツキー（Ｋｃｏｎ）で暗号化したデータであり、Ｅｎｃ（ＫＥＫ，Ｋｃｏｎ）８０２は、コンテンツキー（Ｋｃｏｎ）をコンテンツキー暗号キー（ＫＥＫ：Key Encryption Key）で暗号化したデータであり、Ｅｎｃ（ＥＫＢ，ＫＥＫ）８０３は、コンテンツキー暗号キーＫＥＫを有効化キーブロック（ＥＫＢ）によって暗号化したデータであることを示す。

【００８２】ここで、コンテンツキー暗号キーＫＥＫは、図３で示すノードキー（Ｋ０００，Ｋ００…）、あるいはルートキー（Ｋｒｏｏｔ）自体であってもよく、またノードキー（Ｋ０００，Ｋ００…）、あるいはルートキー（Ｋｒｏｏｔ）によって暗号化されたキーであってもよい。

【００８３】図８（ｂ）は、複数のコンテンツがメディアに記録され、それぞれが同じＥｎｃ（ＥＫＢ，ＫＥＫ）８０５を利用している場合の構成例を示す、このような構成においては、各データに同じＥｎｃ（ＥＫＢ，ＫＥＫ）を付加することなく、Ｅｎｃ（ＥＫＢ，ＫＥＫ）にリンクするリンク先を示すデータを各データに付加する構成とすることができる。

【００８４】図９にコンテンツキー暗号キーＫＥＫを、図３に示すノードキーＫ００を更新した更新ノードキーＫ（ｔ）００として構成した場合の例を示す。この場合、図３の点線枠で囲んだグループにおいてデバイス３が、例えば鍵の漏洩によりリボーク（排除）されているとして、他のグループのメンバ、すなわち、デバイス０，１，２に対して図９に示す（ａ）有効化キーブロック（ＥＫＢ）と、（ｂ）コンテンツキー（Ｋｃｏｎ）をコンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）で暗号化したデータと、（ｃ）コンテンツ（content）をコンテンツキー（Ｋｃｏｎ）で暗号化したデータとを配信することにより、デバイス０，１，２はコンテンツを得ることができる。

【００８５】図９の右側には、デバイス０における復号手順を示してある。デバイス０は、まず、受領した有効化キーブロックから自身の保有するリーフキーＫ０００を用いた復号処理により、コンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）を取得する。次に、Ｋ（ｔ）００

による復号によりコンテンツキーＫｃｏｎを取得し、さらにコンテンツキーＫｃｏｎによりコンテンツの復号を行なう。これらの処理により、デバイス０はコンテンツを利用可能となる。デバイス１，２においても各々異なる処理手順でＥＫＢを処理することにより、コンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）を取得することが可能となり、同様にコンテンツを利用することが可能となる。

【００８６】図３に示す他のグループのデバイス４，５，６…は、この同様のデータ（ＥＫＢ）を受信したとしても、自身の保有するリーフキー、ノードキーのセット、すなわちデバイスノードキー（ＤＮＫ）を用いてコンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）を取得することができない。同様にリボークされたデバイス３においても、自身の保有するリーフキー、ノードキーのセット、すなわちデバイスノードキー（ＤＮＫ）では、コンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）を取得することができず、正当な権利を有するデバイスのみがコンテンツを復号して利用することが可能となる。

【００８７】このように、ＥＫＢを利用したコンテンツキーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能とした暗号化コンテンツを配信することが可能となる。

【００８８】なお、有効化キーブロック（ＥＫＢ）、コンテンツキー、暗号化コンテンツ等は、ネットワークを介して安全に配信することが可能な構成であるが、有効化キーブロック（ＥＫＢ）、コンテンツキー、暗号化コンテンツをＤＶＤ、ＣＤ等の記録媒体に格納してユーザに提供することも可能である。この場合、記録媒体に格納された暗号化コンテンツの復号には、同一の記録媒体に格納された有効化キーブロック（ＥＫＢ）の復号により得られるコンテンツキーを使用するように構成すれば、予め正当権利者のみが保有するリーフキー、ノードキーによってのみ利用可能な暗号化コンテンツの配布処理、すなわち利用可能なユーザデバイスを限定したコンテンツ配布が簡易な構成で実現可能となる。

【００８９】図１０に記録媒体に暗号化コンテンツとともに有効化キーブロック（ＥＫＢ）を格納した構成例を示す。図１０に示す例においては、記録媒体にコンテンツＣ１～Ｃ４が格納され、さらに各格納コンテンツに対応するの有効化キーブロック（ＥＫＢ）を対応付けたデータが格納され、さらにバージョンＭの有効化キーブロック（ＥＫＢ＿Ｍ）が格納されている。例えばＥＫＢ＿１はコンテンツＣ１を暗号化したコンテンツキーＫｃｏｎ１を生成するのに使用され、例えばＥＫＢ＿２はコンテンツＣ２を暗号化したコンテンツキーＫｃｏｎ２を生成するのに使用される。この例では、バージョンＭの有効化キーブロック（ＥＫＢ＿Ｍ）が記録媒体に格納されており、コンテンツＣ３，Ｃ４は有効化キーブロック（ＥＫＢ＿Ｍ）に対応付けられているので、有効化キーブロック（ＥＫＢ＿Ｍ）の復号によりコンテンツＣ３，Ｃ４のコンテンツキーを取得することができる。ＥＫＢ＿１、ＥＫＢ＿２はディスクに格納されていないので、新たな提供手段、例えばネットワーク配信、あるいは記録媒体による配信によってそれぞれのコンテンツキーを復号するために必要なＥＫＢ＿１，ＥＫＢ＿２を取得することが必要となる。

【００９０】［階層ツリー構造のカテゴリー分類］上述したように、ルートキー、ノードキー、リーフキーからなる図３の階層ツリー構造を適用することで、コンテンツ暗号化に適用するコンテンツキーのみならず、相互認証処理に適用する認証キー、通信データの改竄チェック値生成鍵として適用するＩＣＶ（Integrity Check Value）生成キー、あるいはプログラムコード、データ等を有効化キーブロック（ＥＫＢ）とともに暗号化して配信することが可能である。さらに、ノードキー等を定義している階層ツリー構造を各デバイスのカテゴリー毎に分類して効率的なキー更新処理、暗号化キー配信、データ配信を実行する構成について、以下説明する。

【００９１】図１１に階層ツリー構造のカテゴリーの分類の一例を示す。図１１において、階層ツリー構造の最上段には、ルートキーＫｒｏｏｔ，１１０１が設定され、以下の中間段にはノードキー１１０２が設定され、最下段には、リーフキー１１０３が設定される。各デバイスは個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーを保有する。

【００９２】ここで、一例として最上段から第Ｍ段目のあるノードをカテゴリノード１１０４として設定する。すなわち第Ｍ段目のノードの各々を特定カテゴリのデバイス設定ノードとする。第Ｍ段の１つのノードを頂点として以下、Ｍ＋１段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとする。

【００９３】例えば図１１の第Ｍ段目の１つのノード１１０５にはカテゴリ［メモリステッイク（商標）］が設定され、このノード以下に連なるノード、リーフはメモリステッイクを使用した様々なデバイスを含むカテゴリ専用のノードまたはリーフとして設定される。すなわち、ノード１１０５以下を、メモリスティックのカテゴリに定義されるデバイスの関連ノード、およびリーフの集合として定義する。

【００９４】さらに、Ｍ段から数段分下位の段をサブカテゴリノード１１０６として設定することができる。例えば図に示すようにカテゴリ［メモリスティック］ノード１１０５の２段下のノードに、メモリスティックを使用したデバイスのカテゴリに含まれるサブカテゴリノードとして、［再生専用器］のノードを設定する。さらに、サブカテゴリノードである再生専用器のノード１１０６以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード１１０７が設定され、さらにその

下位に、音楽再生機能付き電話のカテゴリに含まれる［ＰＨＳ］ノード１１０８と［携帯電話］ノード１１０９を設定することができる。［ＰＨＳ］ノード１１０８と［携帯電話］ノード１１０９の下位に接続されるリーフに対応するデバイスは、メモリスティックを使用可能なＰＨＳ、または携帯電話である。

【００９５】さらに、カテゴリ、サブカテゴリは、デバイスの種類のみならず、例えばあるメーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位（これらを総称して以下、エンティティと呼ぶ）で設定することが可能である。例えば１つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器ＸＹＺ専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器ＸＹＺにその頂点ノード以下の下段のノードキー、リーフキーを格納して販売することが可能となり、その後、暗号化コンテンツの配信、あるいは各種キーの配信、更新処理を、その頂点ノードキー以下のノードキー、リーフキーによって構成される有効化キーブロック（ＥＫＢ）を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

【００９６】このように、１つのノードを頂点としして、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の１つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化キーブロック（ＥＫＢ）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには全く影響を及ぼさずにキー更新を実行することができる。

【００９７】［簡略ＥＫＢによるキー配信構成］先に説明した例えば図３のツリー構成において、キー、例えばコンテンツキーを所定デバイス（リーフ）宛に送付する場合、キー配布先デバイスの所有しているリーフキー、ノードキーを用いて復号可能な有効化キーブロック（ＥＫＢ）を生成して提供する。例えば図１２（ａ）に示すツリー構成において、リーフを構成するデバイスａ，ｇ，ｊに対してキー、例えばコンテンツキーを送信する場合、ａ，ｇ，ｊの各ノードにおいて復号可能な有効化キーブロック（ＥＫＢ）を生成して配信する。

【００９８】例えば更新ルートキーＫ（ｔ）ｒｏｏｔでコンテンツキーＫ（ｔ）ｃｏｎを暗号化処理し、ＥＫＢとともに配信する場合を考える。この場合、デバイスａ，ｇ，ｊは、それぞれが図１２（ｂ）に示すリーフおよびノードキーを用いて、ＥＫＢの処理を実行してＫ（ｔ）ｒｏｏｔを取得し、取得した更新ルートキーＫ（ｔ）ｒｏｏｔによってコンテンツキーＫ（ｔ）ｃｏｎの復号処理を実行してコンテンツキーを得る。

【００９９】この場合に提供される有効化キーブロック（ＥＫＢ）の構成は、図１３に示すようになる。図１３に示す有効化キーブロック（ＥＫＢ）は、先の図６で説明した有効化キーブロック（ＥＫＢ）のフォーマットにしたがって構成されたものであり、データ（暗号化キー）と対応するタグとを持つ。タグは、先に図７を用いて説明したように左（Ｌ）、右（Ｒ）、それぞれの方向にデータがあれば０、無ければ１を示している。

【０１００】有効化キーブロック（ＥＫＢ）を受領したデバイスは、有効化キーブロック（ＥＫＢ）の暗号化キーとタグに基づいて、順次暗号化キーの復号処理を実行して上位ノードの更新キーを取得していく。図１３に示すように、有効化キーブロック（ＥＫＢ）は、ルートからリーフまでの段数（デプス）が多いほど、そのデータ量は増加していく。段数（デプス）は、デバイス（リーフ）数に応じて増大するものであり、キーの配信先となるデバイス数が多い場合は、ＥＫＢのデータ量がさらに増大することになる。

【０１０１】このような有効化キーブロック（ＥＫＢ）のデータ量の削減を可能とした構成について説明する。図１４は、有効化キーブロック（ＥＫＢ）をキー配信デバイスに応じて簡略化して構成した例を示すものである。

【０１０２】図１３と同様、リーフを構成するデバイスａ，ｇ，ｊに対してキー、例えばコンテンツキーを送信する場合を想定する。図１４の（ａ）に示すように、キー配信デバイスによってのみ構成されるツリーを構築する。この場合、図１２（ｂ）に示す構成に基づいて新たなツリー構成として図１４（ｂ）のツリー構成が構築される。ＫｒｏｏｔからＫｊまでは全く分岐がなく１つの枝のみが存在すればよく、ＫｒｏｏｔからＫａおよびＫｇに至るためには、Ｋ０に分岐点を構成するのみで、２分岐構成の図１４（ａ）のツリーが構築される。

【０１０３】図１４（ａ）に示すように、ノードとしてＫ０のみを持つ簡略化したツリーが生成される。更新キー配信のための有効化キーブロック（ＥＫＢ）は、これらの簡略ツリーに基づいて生成する。図１４（ａ）に示すツリーは、有効化キーブロック（ＥＫＢ）を復号可能な末端ノードまたはリーフを最下段とした２分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーである。更新キー配信のための有効化キーブロック（ＥＫＢ）は、この再構築階層ツリーのノードまたはリーフに対応するキーのみに基づいて構成される。

【０１０４】先の図１３で説明した有効化キーブロック（ＥＫＢ）は、各リーフａ，ｇ，ｊからＫｒｏｏｔに至るまでのすべてのキーを暗号化したデータを格納していたが、簡略化ＥＫＢは、簡略化したツリーを構成するノードについてのみの暗号化データを格納する。図１４

（ｂ）に示すようにタグは３ビット構成を有する。第１および第２ビットは、図１３の例と、同様の意味を持ち、左（Ｌ）、右（Ｒ）、それぞれの方向にデータがあれば０、無ければ１を示す。第３番目のビットは、ＥＫＢ内に暗号化キーが格納されているか否かを示すためのビットであり、データが格納されている場合は１、データが無い場合は、０として設定される。

【０１０５】データ通信網、あるいは記憶媒体に格納されてデバイス（リーフ）に提供される有効化キーブロック（ＥＫＢ）は、図１４（ｂ）に示すように、図１３に示す構成に比較すると、データ量が大幅に削減されたものとなる。図１４に示す有効化キーブロック（ＥＫＢ）を受領した各デバイスは、タグの第３ビットに１が格納された部分のデータのみを順次復号することにより、所定の暗号化キーの復号を実現することができる。例えばデバイスａは、暗号化データＥｎｃ（Ｋａ，Ｋ（ｔ）０）をリーフキーＫａで復号して、ノードキーＫ（ｔ）０を取得して、ノードキーＫ（ｔ）０によって暗号化データＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）ｒｏｏｔ）を復号してＫ（ｔ）ｒｏｏｔを取得する。デバイスｊは、暗号化データＥｎｃ（Ｋｊ，Ｋ（ｔ）ｒｏｏｔ）をリーフキーＫｊで復号して、Ｋ（ｔ）ｒｏｏｔを取得する。

【０１０６】このように、配信先のデバイスによってのみ構成される簡略化した新たなツリー構成を構築して、構築されたツリーを構成するリーフおよびノードのキーのみを用いて有効化キーブロック（ＥＫＢ）を生成することにより、少ないデータ量の有効化キーブロック（ＥＫＢ）を生成することが可能となり、有効化キーブロック（ＥＫＢ）のデータ配信が効率的に実行可能となる。

【０１０７】なお、簡略化した階層ツリー構成は、後段で説明するエンティティ単位のＥＫＢ管理構成において特に有効に活用可能である。エンティティは、キー配信構成としてのツリー構成を構成するノードあるいはリーフから選択した複数のノードあるいはリーフの集合体ブロックである。エンティティは、デバイスの種類に応じて設定される集合であったり、あるいはデバイス提供メーカー、コンテンツプロバイダ、決済機関等の管理単位等、ある共通点を持った処理単位、管轄単位、あるいは提供サービス単位等、様々な態様の集合として設定される。１つのエンティティには、ある共通のカテゴリに分類されるデバイスが集まっており、例えば複数のエンティティの頂点ノード（サブルート）によって上述したと同様の簡略化したツリーを再構築してＥＫＢを生成することにより、選択されたエンティティに属するデバイスにおいて復号可能な簡略化された有効化キーブロック（ＥＫＢ）の生成、配信が可能となる。エンティティ単位の管理構成については後段で詳細に説明する。

【０１０８】なお、このような有効化キーブロック（ＥＫＢ）は、光ディスク、ＤＶＤ等の情報記録媒体に格納した構成とすることが可能である。例えば、上述の暗号化キーデータによって構成されるデータ部と、暗号化キーデータの階層ツリー構造における位置識別データとしてのタグ部とを含む有効化キーブロック（ＥＫＢ）にさらに、更新ノードキーによって暗号化したコンテンツ等のメッセージデータとを格納した情報記録媒体を各デバイスに提供する構成が可能である。デバイスは有効化キーブロック（ＥＫＢ）に含まれる暗号化キーデータをタグ部の識別データにしたがって順次抽出して復号し、コンテンツの復号に必要なキーを取得してコンテンツの利用を行なうことが可能となる。もちろん、有効化キーブロック（ＥＫＢ）をインターネット等のネットワークを介して配信する構成としてもよい。

【０１０９】［リムーバブル記録媒体に対するデータ記録、再生処理］次に、上述した階層ツリー構成を適用した有効化キーブロック（ＥＫＢ）を適用した処理構成において、コンテンツ再生を実行する装置としてのＰＣ，携帯電話、再生装置に対して着脱自在な記録媒体（リムーバブル記憶装置）、例えばメモリスティック等のメモリカードに対するデータ格納処理について説明する。

【０１１０】（情報記録装置および情報再生装置構成）図１５はコンテンツの記録または再生処理を実行する情報記録装置および情報再生装置としてのデータ処理装置の構成例を示すブロック図である。具体的には、ＰＣ、携帯電話、データ再生装置等であり、メモリカード等の記録媒体としてのリムーバブル記憶装置が着脱可能な構成を持つ。

【０１１１】データ処理装置１００は、デジタル信号の入出力処理を行なう入出力Ｉ／Ｆ(Interface)１２０、アナログ信号の入出力処理を行なうＡ／Ｄ，Ｄ／Ａコンバータ１３１を備えた入出力Ｉ／Ｆ(Interface)１３０、暗号処理手段１４０、ＲＯＭ (Read Only Memory) １５０、ＲＡＭ (Random Access Memory) １６０、ＣＰＵ(Central Processing Unit)１７０、内部メモリ１８０、リムーバブル記憶装置２００のドライブ１９０を有し、これらはバス１１０によって相互に接続されている。

【０１１２】入出力Ｉ／Ｆ１２０は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス１１０上に出力するとともに、バス１１０上のデジタル信号を受信し、外部に出力する。入出力Ｉ／Ｆ１３０は、Ａ／Ｄ，Ｄ／Ａコンバータ１３１を内蔵している。入出力Ｉ／Ｆ１３０は、外部から供給されるコンテンツとしてのアナログ信号を受信し、Ａ／Ｄ，Ｄ／Ａコンバータ１３１でＡ／Ｄ(Analog Digital)変換することで、デジタル信号としてバス１１０上に出力するとともに、バス１１０上のデジタル信号を受信し、Ａ／Ｄ，Ｄ／Ａコンバータ１３１でＤ／Ａ(Digital Analog)変換することで、アナログ信号として、外部に出力する。

【０１１３】暗号処理手段１４０は、例えば、１チップ

のＬＳＩ(Large Scale IntegratedCurcuit)で構成され、例えばバス１１０を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス１１０上に出力する処理や、乱数を生成し、生成した乱数に基づく暗号処理鍵を生成する処理など、暗号処理に伴う各種処理を実行する構成を持つ。なお、暗号処理手段１５０は１チップＬＳＩに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能であり、ＣＰＵ１７０の機能によって実行する構成としてもよい。

【０１１４】ＲＯＭ１５０は、ＣＰＵ１７０が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。ＲＡＭ（Random Access Memory）１６０は、ＣＰＵ１７０の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。ＣＰＵ１７０は、ＲＯＭ１５０、内部メモリ１８０等に格納されたプログラムを実行し、暗号処理手段１５０による暗号処理、データの記録再生に伴う各種処理の制御を実行する。

【０１１５】記憶装置Ｉ／Ｆ１９０は、デジタルデータを記録再生可能なリムーバブル記憶装置２００に対するデータ入出力を制御することにより、リムーバブル記憶装置２００からデータを読み出し（再生し）、バス１１０上に出力するとともに、バス１１０を介して供給されるデータを、リムーバブル記憶装置２００に供給して記録する。

【０１１６】このデータ処理装置は、図３を用いて説明したツリー構成のリーフに対応し、リーフキー、ノードキーからなるキーセットとしてのデバイスノードキー（ＤＮＫ）を内部メモリ１８０に格納している。例えば、デバイス０に対応するデータ処理装置であればリーフキーＫ００００と、ノードキー：Ｋ０００、Ｋ００、Ｋ０、Ｋｒｏｏｔとをデバイスノードキー（ＤＮＫ）として内部メモリ１８０に格納している。なお、内部メモリ１８０は、入出力Ｉ／Ｆ１２０，１４０、または記憶装置Ｉ／Ｆを介して外部から入力されるコンテンツの格納領域として、また有効化キーブロック（ＥＫＢ）の格納領域としても使用可能である。

【０１１７】図１５に示すデータ処理装置は、ネットワーク、電話回線、あるいはコンテンツ配信端末等からコンテンツを正規に購入して、内部メモリ１８０に格納し、内部メモリ１８０からコンテンツを読み出して再生処理を行なう。外部から提供されるコンテンツが前述の有効化キーブロック（ＥＫＢ）の処理によって取得可能なコンテンツキーＫｃｏｎを用いて暗号化されたコンテンツであれば、先に図９を用いて説明したように、装置内に格納されたデバイスノードキー（ＤＮＫ）でＥＫＢの復号処理を行ない、取得したコンテンツキーによって暗号化コンテンツを復号した後、再生する。

【０１１８】このようなコンテンツ再生可能なデータ処理装置において、外部から取得し、内部メモリに格納したコンテンツをリムーバブル記憶装置としての例えばメモリカードに出力する場合の処理について説明する。

【０１１９】（コンテンツ格納処理）図１６にデータ処理装置におけるリムーバブル記憶装置に対するコンテンツ格納処理の処理手順を説明する図を示す。図１６に示す例は、データ処理装置が図３のツリー構成におけるデバイス０に対応する場合の処理例である。

【０１２０】まず、データ処理装置は、データ記録媒体としてのリムーバブル記憶装置に格納するコンテンツに対応するＥＫＢを選択し、自己のデバイスノードキー（ＤＮＫ）を用いてＥＫＢの復号処理を実行し、ＥＫＢから階層ツリー構成鍵であるルートキーを取り出す。図の例では、リムーバブル記憶装置に格納するコンテンツに対応するＥＫＢはバージョン：ｔのＥＫＢであり、データ処理装置は、内部メモリからバージョン：ｔのＥＫＢを取得してデバイスノードキー、この場合はＫ０００を用いてＥＫＢの復号を実行してルートキーＫ（ｔ）ｒｏｏｔを取り出す。

【０１２１】次に、データ処理装置は、乱数を発生して乱数に基づくコンテンツキー：Ｋｃｏｎを生成する。このコンテンツキーは、リムーバブル記憶装置に対してコンテンツを格納する際に逐次発生する乱数に基づくものであり、コンテンツの格納処理毎に異なるコンテンツキーが生成されることになる。なお、このコンテンツキーの生成処理は、ネットワーク、またはコンテンツ配信端末等から取得したコンテンツがコンテンツキーを用いて暗号化されていない場合にも適用可能とするための処理であり、外部から取得したコンテンツが予めコンテンツキーによって暗号化されている場合であって、コンテンツキーを外部から取得可能な場合は、この乱数に基づくコンテンツキーの生成処理は省略し、外部から取得したコンテンツキーを適用してもよい。なお、この場合であっても、データ処理装置内で改めて乱数に基づいてコンテンツキーを生成してもよい。

【０１２２】次に、例えば乱数に基づいて生成したコンテンツキーを先にＥＫＢ処理によって取得したルートキー：Ｋ（ｔ）ｒｏｏｔで暗号化して、コンテンツキーのルートキーによる暗号化データ：Ｅｎｃ（Ｋ（ｔ）ｒｏｏｔ，Ｋｃｏｎ）を取得する。

【０１２３】さらに、生成したコンテンツキー：Ｋｃｏｎにより、データ処理装置のＩＤ、例えばデータ処理装置が携帯電話であれば、携帯電話に対応する電話番号を暗号化し、Ｅｎｃ（Ｋｃｏｎ，ＩＤ）により、ストレージキー：Ｋｓｔを生成する。

【０１２４】次に、ＩＤをコンテンツキー：Ｋｃｏｎで暗号化することにより生成したストレージキー：Ｋｓｔを用いてコンテンツ（ＤＡＴＡ）を暗号化して、暗号化コンテンツ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）を生成する。

【０１２５】このようにして生成したコンテンツキー：Ｋｃｏｎのルートキー：Ｋ（ｔ）ｒｏｏｔによる暗号化データ：Ｅｎｃ（Ｋ（ｔ）ｒｏｏｔ，Ｋｃｏｎ）と、コンテンツ（ＤＡＴＡ）のストレージキー：Ｋｓｔによる暗号化データ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）をリムーバブル記憶装置に対する格納データファイルとする。

【０１２６】データ処理装置は、この暗号化コンテンツを含むデータファイルと、対応するＥＫＢファイルを併せてリムーバブル記憶装置に格納する。なお、格納するＥＫＢファイルとデータファイルは相互の対応付けをして格納する。対応付けは、例えば格納するデータファイルにＥＫＢのバージョン情報を付加することにより実行できる。ＥＫＢファイルには先の図６で説明したように予めバージョン情報が付加されている。

【０１２７】図１７にリムーバブル記憶装置に格納されるＥＫＢファイルとデータファイルの構成例を示す。ＥＫＢファイルは、データ処理装置に予め配布されているデバイスノードキー（ＤＮＫ）を用いて階層ツリー構成鍵であるルートキー：Ｋ（ｔ）ｒｏｏｔを取得可能なＥＫＢである。また、データファイルは、図１６を用いて説明したように、コンテンツキー：Ｋｃｏｎのルートキー：Ｋ（ｔ）ｒｏｏｔによる暗号化データ：Ｅｎｃ（Ｋ（ｔ）ｒｏｏｔ，Ｋｃｏｎ）と、コンテンツ（ＤＡＴＡ）のストレージキー：Ｋｓｔによる暗号化データ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）を含み、ＥＫＢバージョン情報、この図の例の場合はバージョン：ｔが記録された構成となっている。リムーバブル記憶装置には、複数のコンテンツが格納される場合があり、それぞれに対応するＥＫＢファイルも併せて格納される。

【０１２８】（データ再生処理）このようなリムーバブル記憶装置（記録媒体）に格納された暗号化コンテンツ（ＤＡＴＡ）を再生する場合の処理について、図１８を用いて説明する。

【０１２９】図１８の処理例は、正当なコンテンツ購入者であり、リムーバブル記憶装置にコンテンツ格納処理を行なったデータ処理装置（デバイス０）におけるコンテンツ再生処理であり、正常なコンテンツ再生処理が行なわれる例を示している。

【０１３０】まず、データ処理装置は、リムーバブル記憶装置に格納されたデータファイルから対応するＥＫＢバージョン情報を取得し、取得したバージョン情報、この例ではバージョン（ｔ）に対応するＥＫＢファイルをリムーバブル記憶装置から取得してデータ処理装置内に格納されたデバイスノードキー（ＤＮＫ）を用いてＥＫＢの復号処理を実行し、階層ツリー構成鍵であるルートキー：Ｋ（ｔ）ｒｏｏｔを取得する。このＥＫＢ復号処理に成功するのは、予めＥＫＢの復号可能なデバイスノードキー（ＤＮＫ）を格納したデバイスのみとなる。

【０１３１】次に、データ処理装置は、リムーバブル記憶装置内のデータファイルからコンテンツキー：Ｋｃｏｎをルートキー：Ｋ（ｔ）ｒｏｏｔで暗号化したデータ：Ｅｎｃ（Ｋ（ｔ）ｒｏｏｔ，Ｋｃｏｎ）を取得して、ＥＫＢ処理によって取得したルートキー：Ｋ（ｔ）ｒｏｏｔを適用した復号処理を実行して、コンテンツキー：Ｋｃｏｎを取得する。

【０１３２】次に、データ処理装置は、例えばデータ処理装置が携帯電話であれば電話番号、あるいはその他の再生装置であれば機器番号などのＩＤを、取得したコンテンツキー：Ｋｃｏｎを適用して暗号化：Ｅｎｃ（Ｋｃｏｎ，ＩＤ）して、ストレージキー：Ｋｓｔを生成する。このストレージキー：Ｋｓｔは、自己のＩＤに基づくものであり、各機器毎に異なるストレージキーが生成されることになる。すなわち他のＩＤを持つ他の機器においてストレージキーを生成した場合、異なるストレージキーが生成される。

【０１３３】次に、データ処理装置は、リムーバブル記憶装置内のデータファイルからコンテンツ（ＤＡＴＡ）のストレージキー：Ｋｓｔによる暗号化データ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）を取り出して、生成したストレージキー：Ｋｓｔを用いて復号処理を実行する。この復号処理に成功するためには、リムーバブル記憶装置に対するコンテンツ格納処理の際に暗号化に適用したストレージキー：Ｋｓｔと同一のストレージキーが生成される必要がある。この図１８に示す例の場合、データ処理装置は、デバイス０であり、リムーバブル記憶装置に対するコンテンツの格納を行なった機器であり、ＩＤが同一であるので、データ格納時と同一のストレージキーの生成が実行され、暗号化コンテンツ：Ｅｎｋ（Ｋｓｔ，ＤＡＴＡ）の復号に成功し、コンテンツの再生が可能となる。

【０１３４】リムーバブル記憶装置にコンテンツの格納処理を行なった機器と異なる機器においてデータ再生を実行しようとしても、ＩＤが異なり、生成されるストレージキーがデータ格納時に適用したストレージキーと異なることになり、暗号化コンテンツ：Ｅｎｋ（Ｋｓｔ，ＤＡＴＡ）の復号が実行できず、コンテンツの再生は不可能となる。

【０１３５】このように、本発明の構成によれば、リムーバブル記憶装置に格納したコンテンツ再生の実行条件として、ＥＫＢ処理によって復号可能なコンテンツキーを取得可能なデバイスであること、さらに、記録処理を行なった同一デバイスであることが必要となる。従って、図３に示すツリー構成の特定のグループに属し、同一のＥＫＢを復号可能な複数のデバイスが存在する場合であっても、リムーバブル記憶装置に格納したコンテンツを再生可能なデバイスは、コンテンツをリムーバブル記憶装置に格納した唯一のデバイスに限定することが可能となる。

【０１３６】（コンテンツ配信端末におけるコンテンツ・ダウンロード処理）上述したコンテンツ格納処理は、

データ処理装置が予め内部メモリに格納したコンテンツをリムーバブル記憶装置に格納する処理を想定して説明したが、例えば、サービスプロバイダが提供し、駅、店舗等に設置されたコンテンツの配信端末にユーザがリムーバブル記憶装置をセットして、コンテンツを購入、すなわちダウンロードした後、そのリムーバブル記憶装置を自己のデータ処理装置（ＰＣ、携帯電話、再生装置など）にセットしてコンテンツを再生しようとする場合にも、上述の処理と同様、コンテンツを購入した機器において再生可能な構成が実現される。

【０１３７】図１９を用いてコンテンツの配信端末にユーザが記録媒体としてのリムーバブル記憶装置をセットして、コンテンツを購入する処理について説明する。

【０１３８】図１９には、例えばサービスプロバイダが提供し、駅、店舗等に設置されたコンテンツの配信端末３００と、コンテンツの配信端末３００からコンテンツを購入して再生を実行しようとするデータ処理装置としての携帯電話型の再生装置Ａ，４００と、再生装置Ｂ，５００が示されている。再生装置Ａ，４００と、再生装置Ｂ，５００は、例えばメモリカードのようなリムーバブル記憶装置６００をコンテンツ配信端末３００にセットしてあるコンテンツを選択して購入、すなわち、リムーバブル記憶装置６００に選択コンテンツをダウンロードする処理を実行する。

【０１３９】コンテンツ配信端末３００の構成について説明する。コンテンツ配信端末は、先に図３他を用いて説明したツリー構成の１つのリーフに対応するデータ処理装置（デバイス）として設定され、対応リーフに設定されるデバイスノードキー（ＤＮＫ）を記憶手段３７０に格納し、メモリカード等のリムーバブル記憶装置６００が着脱可能な構成を持つ。

【０１４０】コンテンツ配信端末３００は、データ入出力処理を行なう入出力Ｉ／Ｆ(Interface)３２０、暗号処理手段３３０、ＲＯＭ (Read Only Memory) ３４０、ＲＡＭ (Random Access Memory) ３５０、ＣＰＵ(Central Processing Unit)３６０、記憶手段３７０、リムーバブル記憶装置Ｉ／Ｆ(Interface)３８０を有し、これらはバスによって相互に接続されている。

【０１４１】入出力Ｉ／Ｆ３２０は、例えばダウンロード可能なコンテンツ情報、価格情報等を表示し、またユーザからのコンテンツ購入処理に伴うデータ入力を処理する。暗号処理手段３３０は、例えば、１チップのＬＳＩ(Large Scale IntegratedCurcuit)で構成され、例えばバスを介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス上に出力する処理や、乱数を生成し、生成した乱数に基づく暗号処理鍵を生成する処理など、暗号処理に伴う各種処理を実行する構成を持つ。なお、暗号処理手段３３０は１チップＬＳＩに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能であり、制御手段（ＣＰＵ）３６０の機能によって実行する構成としてもよい。

【０１４２】ＲＯＭ３４０は、制御手段（ＣＰＵ）３６０が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。ＲＡＭ (Random Access Memory) ３５０は、制御手段（ＣＰＵ）３６０の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。制御手段（ＣＰＵ）３６０は、ＲＯＭ３４０、記憶手段３７０等に格納されたプログラムを実行し、暗号処理手段３３０による暗号処理、データのダウンロード処理に伴う各種処理の制御を実行する。

【０１４３】記憶装置Ｉ／Ｆ３８０は、リムーバブル記憶装置２００に対するデータ入出力を制御する。このコンテンツ配信端末３００は、図３を用いて説明したツリー構成のリーフに対応し、リーフキー、ノードキーからなるキーセットとしてのデバイスノードキー（ＤＮＫ）を記憶手段３７０に格納している。例えば、デバイス０に対応するコンテンツ配信端末３００であればリーフキーＫ００００と、ノードキー：Ｋ０００、Ｋ００、Ｋ０、Ｋｒｏｏｔとをデバイスノードキー（ＤＮＫ）として記憶手段３７０に格納している。なお、記憶手段３７０は、コンテンツの格納領域として、また有効化キーブロック（ＥＫＢ）の格納領域としても使用される。

【０１４４】図１９に示すコンテンツ配信端末３００にリムーバブル記憶装置６００をセットし、コンテンツの購入を行なう場合の処理について説明する。

【０１４５】例えば再生装置Ａ，４００を利用して購入コンテンツの再生を行なおうとするユーザは、コンテンツのダウンロードを実行させるリムーバブル記憶装置６００をコンテンツ配信端末３００にセットする。

【０１４６】次に、コンテンツ購入ユーザは、入出力Ｉ／Ｆ３２０を介して、コンテンツを指定し、さらに、再生装置Ａ，４００のＩＤとしての例えば電話番号等、機器に固有の識別データを入力する。

【０１４７】コンテンツ配信端末３００の処理は、先に図１６を用いて説明した処理とほぼ同様の処理となり、図１７に示すようにＥＫＢファイルとデータファイルがリムーバブル記憶装置に格納される。図１６を参照しながら、コンテンツ配信端末３００のリムーバブル記憶装置６００に対するデータ格納処理について説明する。

【０１４８】コンテンツ配信端末３００は、図３のツリー構成におけるデバイス０に対応するものとして説明する。なお、再生装置Ａ，４００もまた、図３のツリー構成におけるいずれかのリーフに対応するデバイスであり、内部にデバイスノードキー（ＤＮＫ）を格納している。

【０１４９】まず、コンテンツ配信端末３００は、ユーザが入出力Ｉ／Ｆ３２０を介して指定したコンテンツに対応するＥＫＢを選択し、自己のデバイスノードキー

（ＤＮＫ）を用いてＥＫＢの復号処理を実行し、ＥＫＢから階層ツリー構成鍵であるルートキーを取り出す。図１６の例では、リムーバブル記憶装置に格納するコンテンツに対応するＥＫＢはバージョン：ｔのＥＫＢであり、コンテンツ配信端末３００は、記憶手段３７０からバージョン：ｔのＥＫＢを取得してデバイスノードキー、この場合はＫ０００を用いてＥＫＢの復号を実行してルートキーＫ（ｔ）ｒｏｏｔを取り出す。

【０１５０】次に、コンテンツ配信端末３００は、暗号処理手段３３０において乱数を発生して乱数に基づくコンテンツキー：Ｋｃｏｎを生成する。このコンテンツキーは、リムーバブル記憶装置に対してコンテンツを格納する際に逐次発生する乱数に基づくものであり、コンテンツのリムーバブル記憶装置に対するダウンロード処理毎に異なるコンテンツキーが生成されることになる。なお、前述したように、このコンテンツキーの生成処理は、コンテンツがコンテンツキーを用いて暗号化されていない場合にも適用可能とするための処理であり、コンテンツが予めコンテンツキーによって暗号化されている場合であって、コンテンツキーを外部から取得済みである場合は、この乱数に基づくコンテンツキーの生成処理は省略し、外部から取得したコンテンツキーを適用してもよい。なお、この場合であっても、コンテンツ配信端末３００内で改めて乱数に基づいてコンテンツキーを生成してもよい。

【０１５１】さらに、乱数に基づいて生成したコンテンツキーを先にＥＫＢ処理によって取得したルートキー：Ｋ（ｔ）ｒｏｏｔで暗号化して、コンテンツキーのルートキーによる暗号化データ：Ｅｎｃ（Ｋ（ｔ）ｒｏｏｔ，Ｋｃｏｎ）を生成する。

【０１５２】さらに、生成したコンテンツキー：Ｋｃｏｎにより、入出力Ｉ／Ｆ３２０を介してユーザにより入力されたコンテンツ購入機器、この例では再生装置Ａ，４００のＩＤとしての携帯電話に対応する電話番号を暗号化し、Ｅｎｃ（Ｋｃｏｎ，ＩＤ）により、ストレージキー：Ｋｓｔを生成する。

【０１５３】次に、ＩＤをコンテンツキー：Ｋｃｏｎで暗号化することにより生成したストレージキー：Ｋｓｔを用いてコンテンツ（ＤＡＴＡ）を暗号化して、暗号化コンテンツ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）を生成する。

【０１５４】このようにして生成したコンテンツキー：Ｋｃｏｎのルートキー：Ｋ（ｔ）ｒｏｏｔによる暗号化データ：Ｅｎｃ（Ｋ（ｔ）ｒｏｏｔ，Ｋｃｏｎ）と、コンテンツ（ＤＡＴＡ）のストレージキー：Ｋｓｔによる暗号化データ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）をリムーバブル記憶装置に対する格納データファイルとする。

【０１５５】コンテンツ配信端末３００は、この暗号化コンテンツを含むデータファイルと、対応するＥＫＢファイルを併せてリムーバブル記憶装置に格納する。なお、格納するＥＫＢファイルとデータファイルは相互の対応付けをして格納する。対応付けは、例えば格納するデータファイルにＥＫＢのバージョン情報を付加することにより実行できる。ＥＫＢファイルには先の図６で説明したように予めバージョン情報が付加されている。

【０１５６】このように、コンテンツ配信端末３００は、外部から入力されたＩＤに基づいてストレージキー：Ｋｓｔを生成し、生成したストレージキー：ｋｓｔを用いてコンテンツを暗号化する。リムーバブル記憶装置に格納されるＥＫＢファイルとデータファイルの構成は、先に説明した図１７の構成と同様であり、ＥＫＢファイルとデータファイルが対応付けられて格納される。

【０１５７】このように、コンテンツ配信端末３００からリムーバブル記憶装置６００に格納された暗号化コンテンツ（ＤＡＴＡ）を再生する場合の処理は、先に説明した図１８の処理と同様である。

【０１５８】ただし、図１８の処理例は、図３のツリー構成のデバイスにおけるデバイス０の処理例であり、コンテンツ配信端末３００がデバイス０に相当すると仮定した場合、再生装置Ａ，４００はデバイス０ではなく、例えばデバイス１であり、この場合、その処理は、リムーバブル記憶装置に格納されたデータファイルから対応するＥＫＢバージョン情報を取得し、取得したバージョン情報、この例ではバージョン（ｔ）に対応するＥＫＢファイルをリムーバブル記憶装置から取得して再生装置Ａ，４００に格納されたデバイスノードキー（ＤＮＫ）を用いてＥＫＢの復号処理を実行し、ルートキー：Ｋ（ｔ）を取得する。このＥＫＢ復号処理に成功するのは、予めＥＫＢの復号可能なデバイスノードキー（ＤＮＫ）を格納したデバイスである。

【０１５９】次に、再生装置Ａ，４００は、リムーバブル記憶装置内のデータファイルからコンテンツキー：Ｋｃｏｎをルートキー：Ｋ（ｔ）ｒｏｏｔで暗号化したデータ：Ｅｎｃ（Ｋ（ｔ）ｒｏｏｔ，Ｋｃｏｎ）を取得して、ＥＫＢ処理によって取得したルートキー：Ｋ（ｔ）ｒｏｏｔを適用した復号処理を実行して、コンテンツキー：Ｋｃｏｎを取得する。

【０１６０】次に、再生装置Ａ，４００はＩＤ、すなわち電話番号を、取得したコンテンツキー：Ｋｃｏｎにより暗号化：Ｅｎｃ（Ｋｃｏｎ，ＩＤ）して、ストレージキー：Ｋｓｔを生成する。このストレージキー：Ｋｓｔは、コンテンツの購入時にコンテンツ配信端末３００が、ユーザから入力されたＩＤに基づいて生成したストレージキー：Ｋｓｔと同一のものとなる。

【０１６１】次に、再生装置Ａ，４００は、リムーバブル記憶装置内のデータファイルからコンテンツ（ＤＡＴＡ）のストレージキー：Ｋｓｔによる暗号化データ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）を取り出して、生成したストレージキー：Ｋｓｔを用いて復号処理を実行する。この復号処理に成功するためには、リムーバブル記憶装置に対するコンテンツ格納処理の際に暗号化に適用したスト

レージキー：Ｋｓｔと同一のストレージキーが生成される必要がある。この場合、コンテンツの格納時と、再生時に適用されるＩＤは再生装置Ａ，４００の電話番号であり、ＩＤが同一であるので、データ格納時と同一のストレージキーの生成が実行され、暗号化コンテンツ：Ｅｎｋ（Ｋｓｔ，ＤＡＴＡ）の復号に成功し、コンテンツの再生が可能となる。

【０１６２】リムーバブル記憶装置にコンテンツの格納処理を行なった機器と異なる機器においてデータ再生を実行しようとした場合、例えば、図１９に示す再生装置Ｂ，５００が、リムーバブル記憶装置６００を借り受けて、再生装置Ｂ，５００にセットして再生を実行しようとしても、再生装置Ｂ，５００では異なるＩＤ（例えば機器番号）に基づいてストレージキーが生成されることになり、生成されたストレージキーは、コンテンツ配信端末３００が、リムーバブル記憶装置６００にコンテンツを暗号化し格納した際に適用したストレージキーと異なるものとなり、復号処理が実行できず、再生処理が不可能となる。

【０１６３】このように、本発明の構成によれば、外部のコンテンツ配信端末からリムーバブル記憶装置に格納したコンテンツの再生を実行する条件として、ＥＫＢ処理によって復号可能なコンテンツキーを取得可能なデバイスであることに加え、さらに、コンテンツ購入処理の際、指定した機器と同一デバイスであることが条件として設定される。従って、図３に示すツリー構成の特定のグループに属し、同一のＥＫＢを復号可能な複数のデバイスが存在する場合であっても、リムーバブル記憶装置に格納したコンテンツを再生可能なデバイスは、コンテンツ購入時に指定した唯一のデバイスに限定することが可能となる。

【０１６４】（コンテンツ記録、再生処理シーケンス）次に、リムーバブル記憶装置に対するコンテンツの格納処理、およびリムーバブル記憶装置に格納されたコンテンツの再生処理についてフローを用いて処理手順を説明する。

【０１６５】まず、図２０の処理フローに従って、リムーバブル記憶装置を着脱可能なデータ処理装置が、内部メモリに格納したコンテンツをリムーバブル記憶装置に格納する処理手順について説明する。

【０１６６】まず、ステップＳ５００１において、リムーバブル記憶装置に格納するコンテンツに適用するＥＫＢファイルを選択する。データ処理装置は、基本的には最新バージョンのＥＫＢファイルのみを格納していればよいが、例えば複数のＥＫＢファイルを格納している場合には、それらのＥＫＢファイルから最新のＥＫＢを選択する。

【０１６７】次に、ステップＳ５００２において、装置内に格納されているリーフキー、ノードキーのキーセットであるデバイスノードキー（ＤＮＫ）を用いてＥＫＢの復号処理を実行して階層ツリー構成鍵であるルートキーＫｒｏｏｔを取得する。

【０１６８】次に、ステップＳ５００３において、乱数を発生し、コンテンツキー：Ｋｃｏｎを生成する。なお、このコンテンツキーの生成処理は、ネットワーク、またはコンテンツ配信端末等から取得したコンテンツがコンテンツキーを用いて暗号化されていない場合にも適用可能とするための処理であり、外部から取得したコンテンツが予めコンテンツキーによって暗号化されている場合であって、コンテンツキーを外部から取得可能な場合は、この乱数に基づくコンテンツキーの生成処理は省略し、外部から取得したコンテンツキーを適用してもよい。なお、この場合であっても、データ処理装置内で改めて乱数に基づいてコンテンツキーを生成してもよい。

【０１６９】次にステップＳ５００４において、ＩＤを内部メモリから取得し、暗号処理手段においてＩＤのコンテンツキー：Ｋｃｏｎによる暗号化：Ｅｎｃ（Ｋｃｏｎ，ＩＤ）を実行してストレージキー：Ｋｓｔを生成（Ｓ５００５）する。

【０１７０】さらに、ステップＳ５００６において、ＥＫＢ処理によって取得したルートキー：Ｋｒｏｏｔにより、コンテンツキー：Ｋｃｏｎの暗号化処理を実行してＥｎｃ（Ｋｒｏｏｔ，Ｋｃｏｎ）を生成する。

【０１７１】さらに、ステップＳ５００７において、リムーバブル記憶装置に格納するコンテンツ（ＤＡＴＡ）をストレージキー：Ｋｓｔで暗号化処理を実行してＥｎｃ（Ｋｓｔ，ＤＡＴＡ）を生成し、ステップＳ５００８において、ＥＫＢファイルと、Ｅｎｃ（Ｋｒｏｏｔ，Ｋｃｏｎ）、Ｅｎｃ（Ｋｒｏｏｔ，Ｋｃｏｎ）を格納したデータファイルとを対応付けてリムーバブル記憶装置に格納する。

【０１７２】次に、図２１の処理フローに従って、コンテンツ配信端末が、コンテンツをユーザのセットしたリムーバブル記憶装置に格納する処理手順について説明する。

【０１７３】まず、ステップＳ６００１において、ユーザのセットしたリムーバブル記憶装置に格納するユーザ指定のコンテンツに適用するＥＫＢファイルを選択する。次に、ステップＳ６００２において、装置内に格納されているリーフキー、ノードキーのキーセットであるデバイスノードキー（ＤＮＫ）を用いてＥＫＢの復号処理を実行して階層ツリー構成鍵であるルートキーＫｒｏｏｔを取得する。

【０１７４】次に、ステップＳ６００３において、乱数を発生し、コンテンツキー：Ｋｃｏｎを生成する。なお、前述したように、このコンテンツキーの生成処理は、コンテンツがコンテンツキーを用いて暗号化されていない場合にも適用可能とするための処理であり、コンテンツが予めコンテンツキーによって暗号化されている場合であって、コンテンツキーを外部から取得済みであ

る場合は、この乱数に基づくコンテンツキーの生成処理は省略し、外部から取得したコンテンツキーを適用してもよい。なお、この場合であっても、コンテンツ配信端末内で改めて乱数に基づいてコンテンツキーを生成してもよい。

【０１７５】次にステップＳ６００４において、ユーザによって外部から入力されるＩＤを取得し、暗号処理手段においてＩＤのコンテンツキー：Ｋｃｏｎによる暗号化：Ｅｎｃ（Ｋｃｏｎ，ＩＤ）を実行してストレージキー：Ｋｓｔを生成（Ｓ６００５）する。

【０１７６】さらに、ステップＳ６００６において、ＥＫＢ処理によって取得したルートキー：Ｋｒｏｏｔにより、コンテンツキー：Ｋｃｏｎの暗号化処理を実行してＥｎｃ（Ｋｒｏｏｔ，Ｋｃｏｎ）を生成する。

【０１７７】さらに、ステップＳ６００７において、リムーバブル記憶装置に格納するコンテンツ（ＤＡＴＡ）をストレージキー：Ｋｓｔで暗号化処理を実行してＥｎｃ（Ｋｓｔ，ＤＡＴＡ）を生成し、ステップＳ６００８において、ＥＫＢファイルと、Ｅｎｃ（Ｋｒｏｏｔ，Ｋｃｏｎ）、Ｅｎｃ（Ｋｒｏｏｔ，Ｋｃｏｎ）を格納したデータファイルとを対応付けてリムーバブル記憶装置に格納する。

【０１７８】次に、図２２の処理フローに従って、リムーバブル記憶装置を着脱可能なデータ処理装置が、リムーバブル記憶装置に格納したコンテンツを再生する処理手順について説明する。

【０１７９】まず、ステップＳ７００１において、リムーバブル記憶装置から再生するコンテンツに適用するＥＫＢファイルを選択する。ＥＫＢファイルの選択は、先に説明した図１７に示す暗号化コンテンツを含むデータファイルに付加されたＥＫＢバージョン情報に一致するＥＫＢファイルをリムーバブル記憶装置から取得する処理として実行される。ステップＳ７００２において、ＥＫＢ取得に成功した場合は、次ステップに進み、ＥＫＢが取得できない場合は、エラー（Ｓ７０１１）として処理は終了する。

【０１８０】次に、ステップＳ７００３において、装置内に格納されているリーフキー、ノードキーのキーセットであるデバイスノードキー（ＤＮＫ）を用いて、リムーバブル記憶装置から取得したＥＫＢの復号処理を実行して階層ツリー構成鍵であるルートキーＫｒｏｏｔを取得する。ルートキーＫｒｏｏｔ取得に成功した場合は、次ステップに進み、ルートキーＫｒｏｏｔが取得できない場合は、エラー（Ｓ７０１１）として処理は終了する。ルートキーＫｒｏｏｔが取得できない場合は、その装置がリボークされている場合などである。

【０１８１】次に、ステップＳ７００５において、リムーバブル記憶装置の格納データファイルから暗号化コンテンツ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）を読み出す。次に、リムーバブル記憶装置の格納データファイルから暗号化コンテンツキー：Ｅｎｃ（Ｋｒｏｏｔ，Ｋｃｏｎ）を読み出して、ステップＳ７００３でのＥＫＢ復号処理により取得したルートキーＫｒｏｏｔで復号処理を行ない、コンテンツキーＫｃｏｎを得る（Ｓ７００６）。

【０１８２】次に、ステップＳ７００７において、自己のＩＤに対するコンテンツキーによる暗号化：Ｅｎｃ（Ｋｃｏｎ，ＩＤ）を実行してストレージキー：Ｋｓｔを生成する。次に、ステップＳ７００８において、リムーバブル記憶装置の格納データファイル読み出した暗号化コンテンツ：Ｅｎｃ（Ｋｓｔ，ＤＡＴＡ）を、生成したストレージキー：Ｋｓｔを適用して復号処理を実行する。

【０１８３】ステップＳ７００９において復号が成功したと判定されると、ステップＳ７０１０で再生を行なう。ステップＳ７００９において復号失敗の場合は、エラー（Ｓ７０１１）として処理は終了する。ステップＳ７００７においてＩＤに基づいて生成したストレージキーと、リムーバブル記憶装置に対するコンテンツ格納処理において適用したストレージキーが異なる場合は、エラーとなる。ストレージキー生成に適用されるＩＤが異なる場合は、再生が実行不可能となる。

【０１８４】なお、上記実施例の説明の中では、説明を省略したが、リムーバブル記憶装置がデータ処理機能を有する場合は、再生装置としてのデータ処理装置あるいはコンテンツ配信端末と、リムーバブル記憶装置との間のデータ入出力に先立ち、両装置間の相互認証処理を実行し、相互認証の成立を条件として、各装置間におけるデータ入出力を実行する構成としてもよい。

【０１８５】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１８６】なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【０１８７】例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（Read OnlyMemory)に予め記録しておくことができる。あるいは、プログラムはフロッピー（登録商標）ディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導

体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０１８８】なお、プログラムは、上述したような記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【０１８９】なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【０１９０】

【発明の効果】以上、説明したように、本発明の情報記録装置、情報再生装置、および情報記録方法、情報再生方法によれば、メモリカードのようなリムーバブル記憶装置に格納したコンテンツの再生を実行する条件として、有効化キーブロック（ＥＫＢ）処理によって復号可能なコンテンツキーを取得可能なデバイスであることに加え、さらに、リムーバブル記憶装置に対する記録処理を行なった同一デバイスであることが条件として設定可能となり、同一のＥＫＢを復号可能な複数のデバイスが存在する場合であっても、リムーバブル記憶装置に格納したコンテンツを再生可能なデバイスは、コンテンツをリムーバブル記憶装置に格納した唯一のデバイスに限定することが可能となる。

【０１９１】さらに、本発明の情報記録装置、情報再生装置、および情報記録方法、情報再生方法によれば、外部のコンテンツ配信端末からリムーバブル記憶装置に格納したコンテンツの再生を実行する条件として、ＥＫＢ処理によって復号可能なコンテンツキーを取得可能なデバイスであることに加え、さらに、コンテンツ購入処理の際、指定した機器と同一デバイスであることが条件として設定可能となり、同一のＥＫＢを復号可能な複数のデバイスが存在する場合であっても、リムーバブル記憶装置に格納したコンテンツを再生可能なデバイスは、コンテンツ購入時に指定した唯一のデバイスに限定することが可能となる。

【図面の簡単な説明】

【図１】本発明のシステムの使用概念を説明する図である。

【図２】本発明のシステム構成例およびリムーバブル記憶装置を用いたデータ利用例を示す図である。

【図３】本発明のシステムにおける各種キー、データの暗号化処理について説明するツリー構成図である。

【図４】本発明のシステムにおける各種キー、データの配布に使用される有効化キーブロック（ＥＫＢ）の例を示す図である。

【図５】本発明のシステムにおけるコンテンツキーの有効化キーブロック（ＥＫＢ）を使用した配布例と復号処理例を示す図である。

【図６】本発明のシステムにおける有効化キーブロック（ＥＫＢ）のフォーマット例を示す図である。

【図７】本発明のシステムにおける有効化キーブロック（ＥＫＢ）のタグの構成を説明する図である。

【図８】本発明のシステムにおける有効化キーブロック（ＥＫＢ）と、コンテンツキー、コンテンツを併せて配信するデータ構成例を示す図である。

【図９】本発明のシステムにおける有効化キーブロック（ＥＫＢ）と、コンテンツキー、コンテンツを併せて配信した場合のデバイスでの処理例を示す図である。

【図１０】本発明のシステムにおける有効化キーブロック（ＥＫＢ）とコンテンツを記録媒体に格納した場合の対応について説明する図である。

【図１１】本発明のシステムにおける階層ツリー構造のカテゴリ分類の例を説明する図である。

【図１２】本発明のシステムにおける簡略化有効化キーブロック（ＥＫＢ）の生成過程を説明する図である。

【図１３】本発明のシステムにおける有効化キーブロック（ＥＫＢ）の生成過程を説明する図である。

【図１４】本発明のシステムにおける簡略化有効化キーブロック（ＥＫＢ）を説明する図である。

【図１５】本発明のシステムにおけるデータ再生装置の構成例を示す図である。

【図１６】本発明のシステムにおける、リムーバブル記憶装置に対するデータ格納処理例を示す図である。

【図１７】本発明のシステムにおいて、リムーバブル記憶装置に格納するデータ例を示す図である。

【図１８】本発明のシステムにおいて、リムーバブル記憶装置からのデータ再生処理例を示す図である。

【図１９】本発明のシステムにおいて、コンテンツ配信端末からのリムーバブル記憶装置に対するデータ格納処理例を示す図である。

【図２０】本発明のシステムにおいて、リムーバブル記憶装置にコンテンツを格納する処理フローを示す図である。

【図２１】本発明のシステムにおいて、コンテンツ配信端末からのリムーバブル記憶装置に対するデータ格納処理フローを示す図である。

【図２２】本発明のシステムにおいて、リムーバブル記憶装置からのデータ再生処理フローを示す図である。

【符号の説明】

１０　コンテンツ配信手段

１１　インターネット

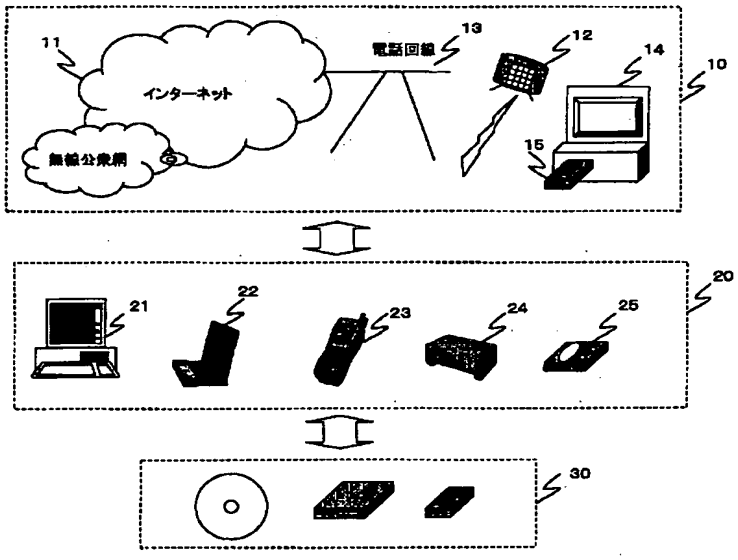
43

１２　衛星放送
１３　電話回線
１４　コンテンツ配信端末
１５　リムーバブル記憶装置
２０　データ処理手段
２１　パーソナルコンピュータ（ＰＣ）
２２　ポータブルデバイス（ＰＤ）
２３　携帯電話、ＰＤＡ
２４　記録再生器、ゲーム端末
２５　再生装置
３０　記憶手段
４０　コンテンツ配信装置
５０　コンテンツ正規購入端末
５１，５２　リムーバブル記憶装置
６０　コンテンツ非正規購入端末
６０１　バージョン
６０２　デプス
６０３　データポインタ
６０４　タグポインタ
６０５　署名ポインタ
６０６　データ部
６０７　タグ部
６０８　署名

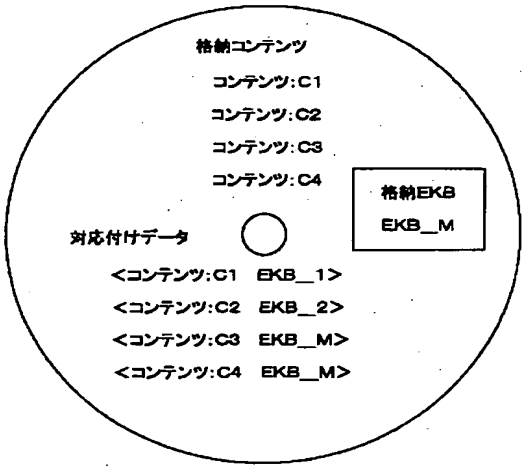
44

＊１００　データ処理装置
１１０　バス
１２０　入出力Ｉ／Ｆ
１３０　入出力Ｉ／Ｆ
１３１　Ａ／Ｄ，Ｄ／Ａコンバータ
１４０　暗号処理手段
１５０　ＲＯＭ
１６０　ＲＡＭ
１７０　ＣＰＵ
１８０　内部メモリ
１９０　記憶装置Ｉ／Ｆ
２００　リムーバブル記憶装置
３００　コンテンツ配信端末
３２０　入出力Ｉ／Ｆ
３３０　暗号処理手段
３４０　ＲＯＭ
３５０　ＲＡＭ
３６０　制御手段（ＣＰＵ）
３７０　記憶手段
３８０　記憶装置Ｉ／Ｆ
４００，５００　再生装置
６００　リムーバブル記憶装置
＊

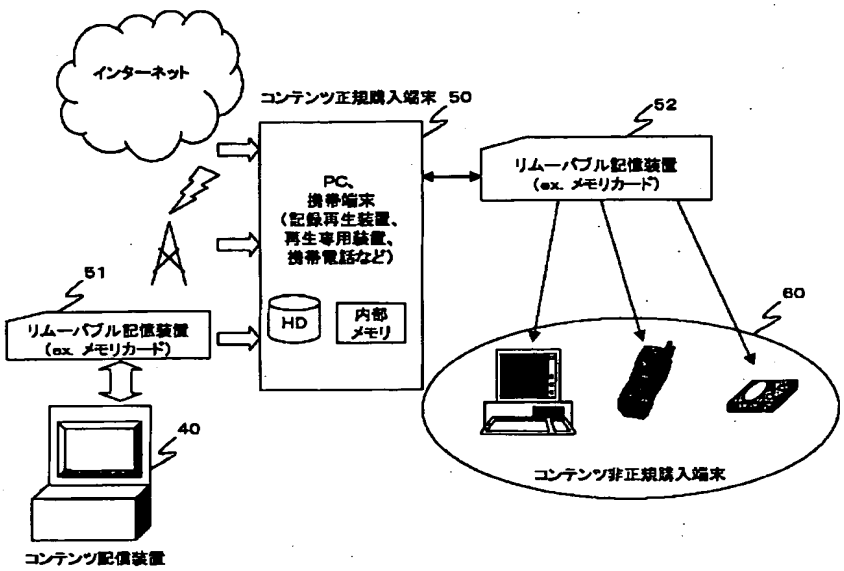
【図１】



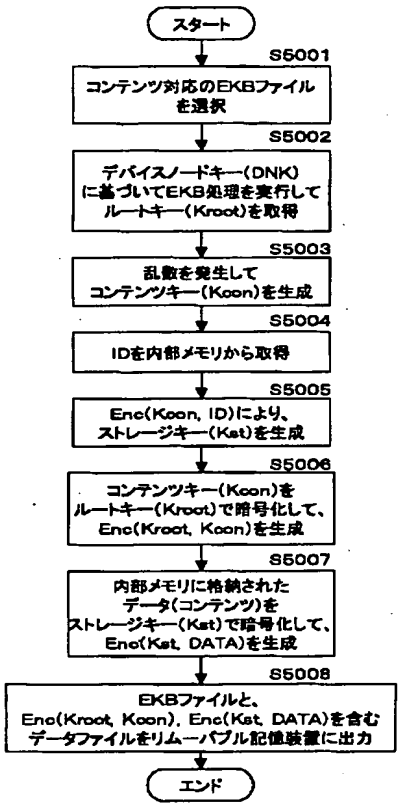
【図１０】



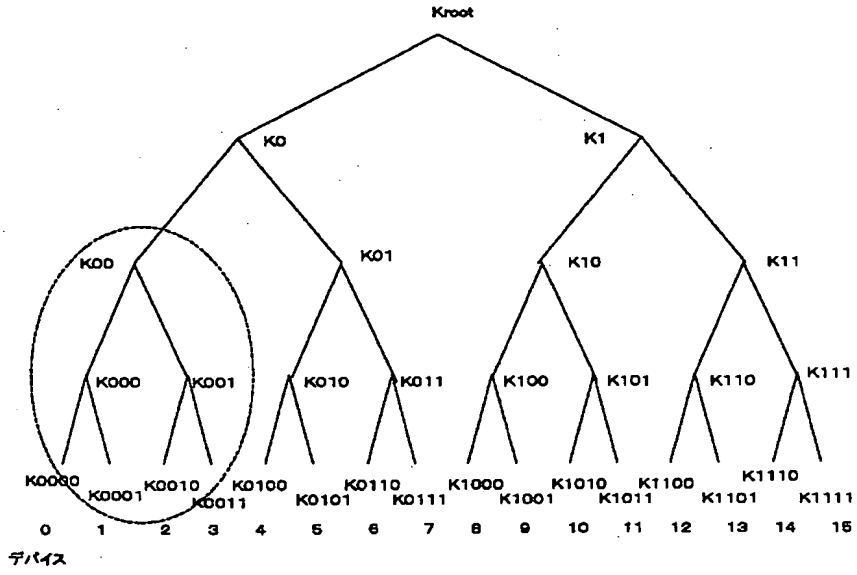
【図２】


インターネット
コンテンツ正規購入端末 50
52
PC、
携帯端末
（記録再生装置、
再生専用装置、
携帯電話など）
リムーバブル記憶装置
（ex. メモリカード）
HD
内部
メモリ
51
リムーバブル記憶装置
（ex. メモリカード）
60
40
コンテンツ非正規購入端末
コンテンツ記憶装置

【図２０】


スタート
S5001
コンテンツ対応のEKBファイル
を選択
S5002
デバイスノードキー（DNK）
に基づいてEKB処理を実行して
ルートキー（Kroot）を取得
S5003
乱数を発生して
コンテンツキー（Kcon）を生成
S5004
IDを内部メモリから取得
S5005
Enc（Kcon, ID）により、
ストレージキー（Kst）を生成
S5006
コンテンツキー（Kcon）を
ルートキー（Kroot）で暗号化して、
Enc（Kroot, Kcon）を生成
S5007
内部メモリに格納された
データ（コンテンツ）を
ストレージキー（Kst）で暗号化して、
Enc（Kst, DATA）を生成
S5008
EKBファイルと、
Enc（Kroot, Kcon）, Enc（Kst, DATA）を含む
データファイルをリムーバブル記憶装置に出力
エンド

【図３】


Kroot
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
デバイス

【図４】

(A) 有効化キーブロック(EKB:Enabling Key Block) 例1

デバイス0, 1, 2にバージョン:tのノードキーを送付

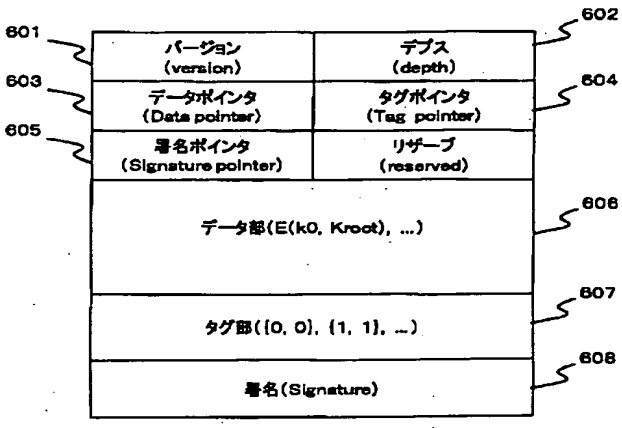
バージョン(Version):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)root)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

(B) 有効化キーブロック(EKB:Enabling Key Block) 例2

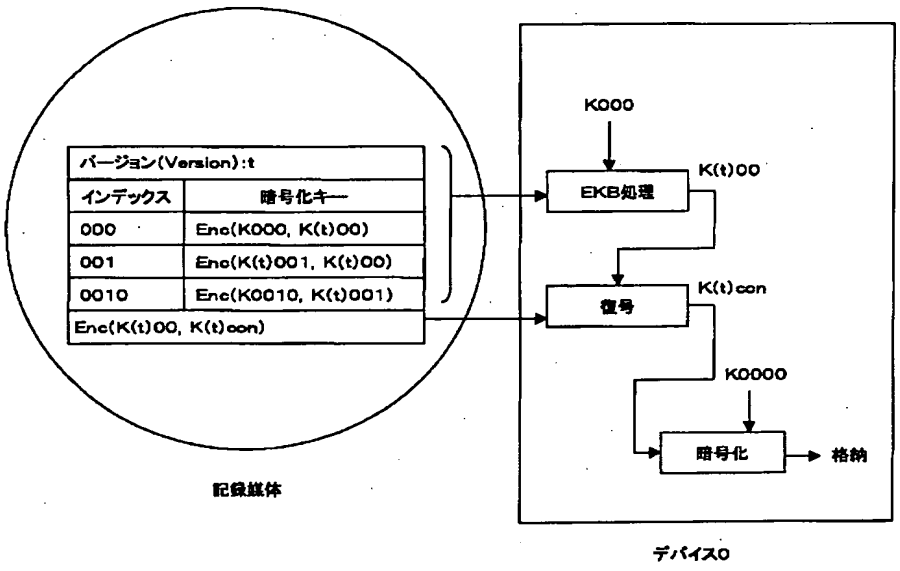
デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

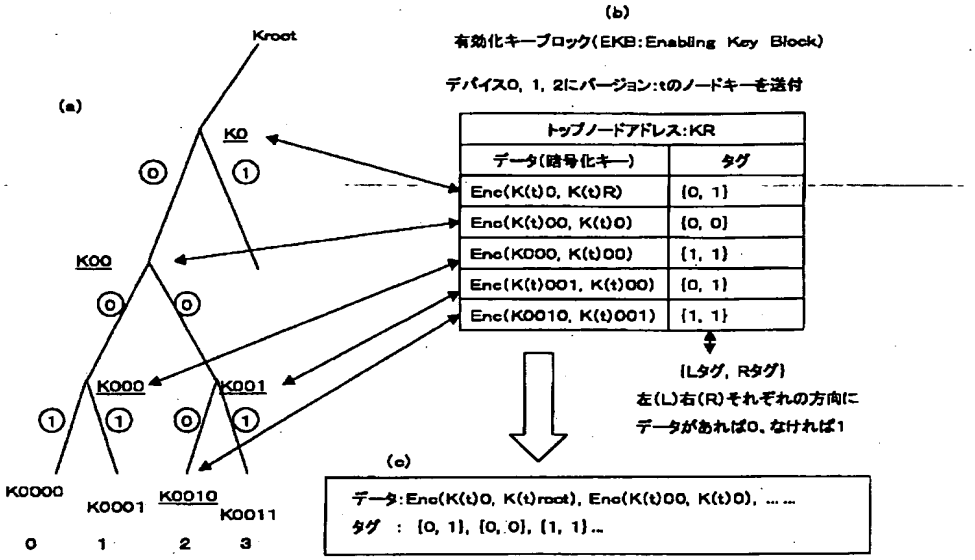
【図６】



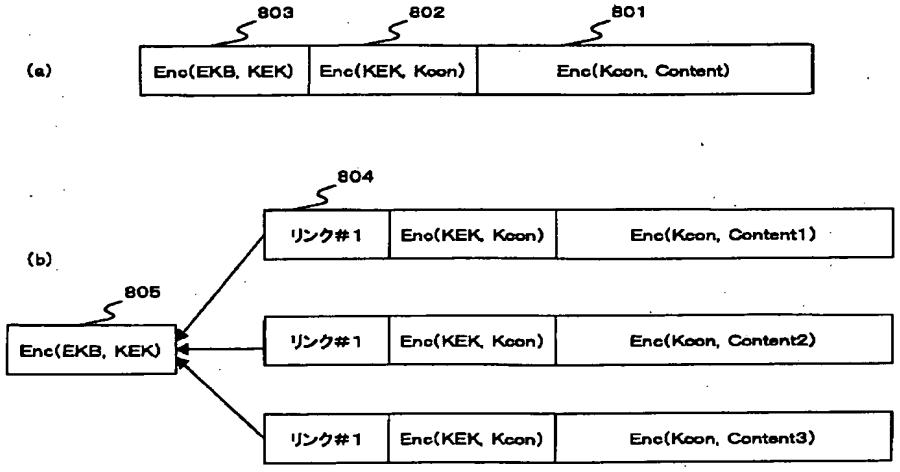
【図５】



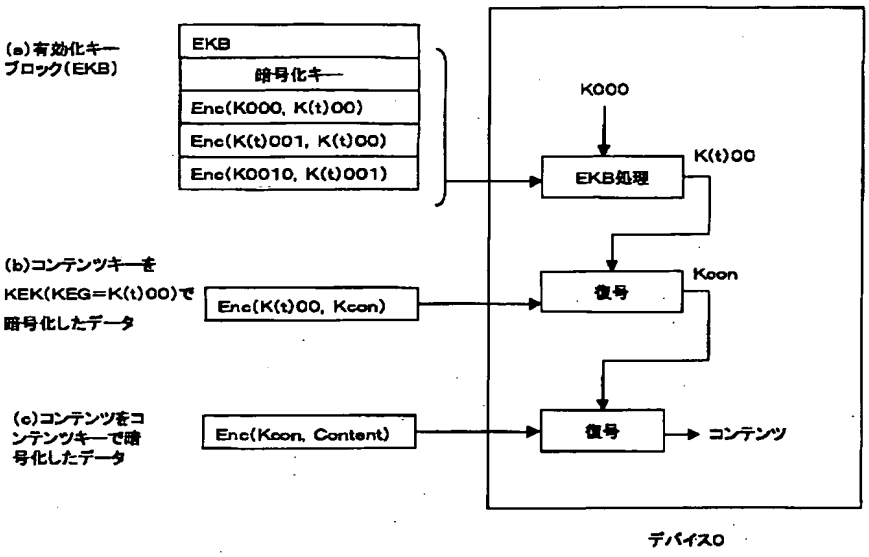
【図７】


(a)
Kroot
K0
K00
K000
K001
K0000
K0001
K0010
K0011
0
1
2
3
(b)
有効化キーブロック(EKB:Enabling Key Block)
デバイス0, 1, 2にバージョン:tのノードキーを送付
トップノードアドレス:KR
データ(暗号化キー)
タグ
Enc(K(t)0, K(t)R)
{0, 1}
Enc(K(t)00, K(t)0)
{0, 0}
Enc(K000, K(t)00)
{1, 1}
Enc(K(t)001, K(t)00)
{0, 1}
Enc(K0010, K(t)001)
{1, 1}
{Lタグ, Rタグ}
左(L)右(R)それぞれの方向に
データがあれば0、なければ1
(c)
データ:Enc(K(t)0, K(t)root), Enc(K(t)00, K(t)0), ……
タグ : {0, 1}, {0, 0}, {1, 1}…

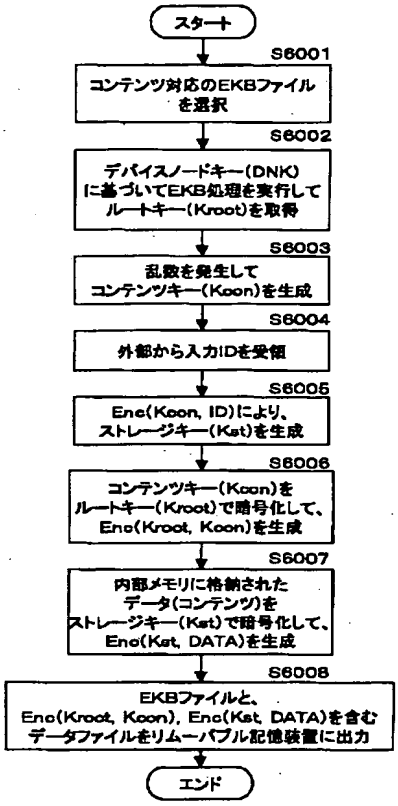
【図８】


(a)
803
802
801
Enc(EKB, KEK)
Enc(KEK, Kcon)
Enc(Kcon, Content)
(b)
804
805
Enc(EKB, KEK)
リンク#1
Enc(KEK, Kcon)
Enc(Kcon, Content1)
リンク#1
Enc(KEK, Kcon)
Enc(Kcon, Content2)
リンク#1
Enc(KEK, Kcon)
Enc(Kcon, Content3)

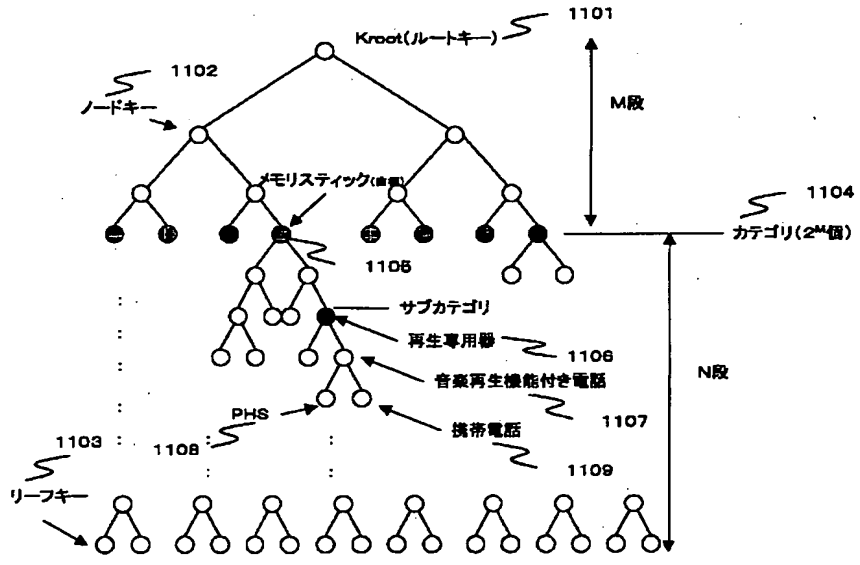
【図９】


(a)有効化キーブロック(EKB)
EKB
暗号化キー
Enc(K000, K(t)00)
Enc(K(t)001, K(t)00)
Enc(K0010, K(t)001)
K000
K(t)00
EKB処理
(b)コンテンツキーをKEK(KEG=K(t)00)で暗号化したデータ
Enc(K(t)00, Kcon)
Kcon
復号
(c)コンテンツをコンテンツキーで暗号化したデータ
Enc(Kcon, Content)
復号
コンテンツ
デバイス0

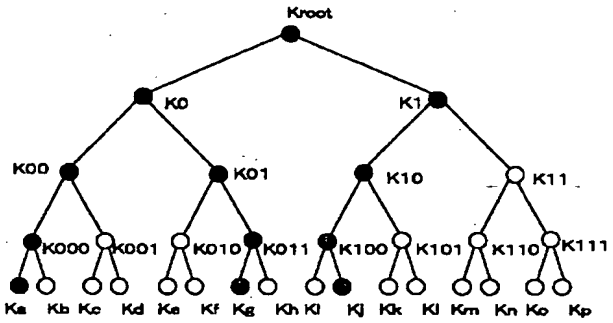
【図２１】


スタート
S6001
コンテンツ対応のEKBファイルを選択
S6002
デバイスノードキー(DNK)に基づいてEKB処理を実行してルートキー(Kroot)を取得
S6003
乱数を発生してコンテンツキー(Kcon)を生成
S6004
外部から入力IDを受領
S6005
Enc(Kcon, ID)により、ストレージキー(Kst)を生成
S6006
コンテンツキー(Kcon)をルートキー(Kroot)で暗号化して、Enc(Kroot, Kcon)を生成
S6007
内部メモリに格納されたデータ(コンテンツ)をストレージキー(Kst)で暗号化して、Enc(Kst, DATA)を生成
S6008
EKBファイルと、Enc(Kroot, Kcon), Enc(Kst, DATA)を含むデータファイルをリムーバブル記憶装置に出力
エンド

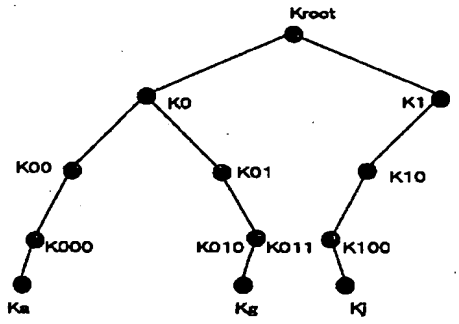
【図１１】


1101
Kroot(ルートキー)
1102
ノードキー
M段
メモリスティック(登録商標)
1104
カテゴリ(2^M個)
1105
サブカテゴリ
再生専用機
1106
音楽再生機能付き電話
1107
携帯電話
1108
PHS
1109
1103
リーフキー
N段

【図１２】



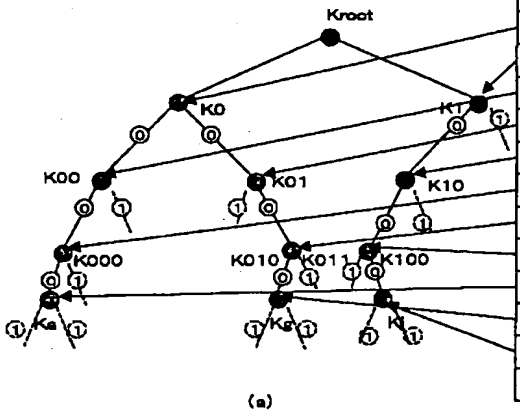
(a)



(b)

【図１３】

有効化キーブロック(EKB:Enabling Key Block)を用いた
デバイスKa, Kg, Kjへのバージョンｔのコンテンツキー送付処理



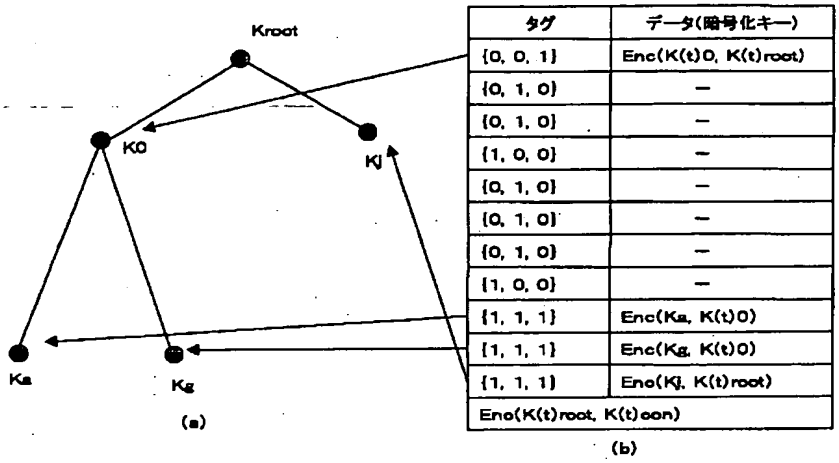
(a)

タグ	データ(暗号化キー)
{0, 0}	Enc(K(t)0, K(t)root)
{0, 1}	Enc(K(t)1, K(t)root)
{0, 1}	Enc(K(t)00, K(t)0)
{1, 0}	Enc(K(t)01, K(t)0)
{0, 1}	Enc(K(t)10, K(t)1)
{0, 1}	Enc(K(t)000, K(t)00)
{0, 1}	Enc(K(t)011, K(t)01)
{1, 0}	Enc(K(t)100, K(t)10)
{1, 1}	Enc(Ka, K(t)000)
{1, 1}	Enc(Kg, K(t)011)
{1, 1}	Enc(Kj, K(t)100)
Enc(K(t)root, K(t)con)	

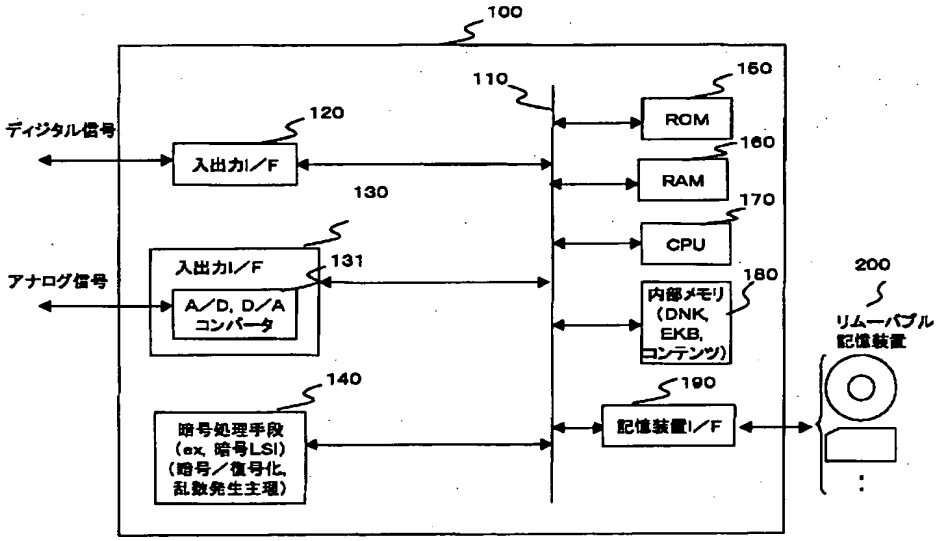
(b)

【図１４】

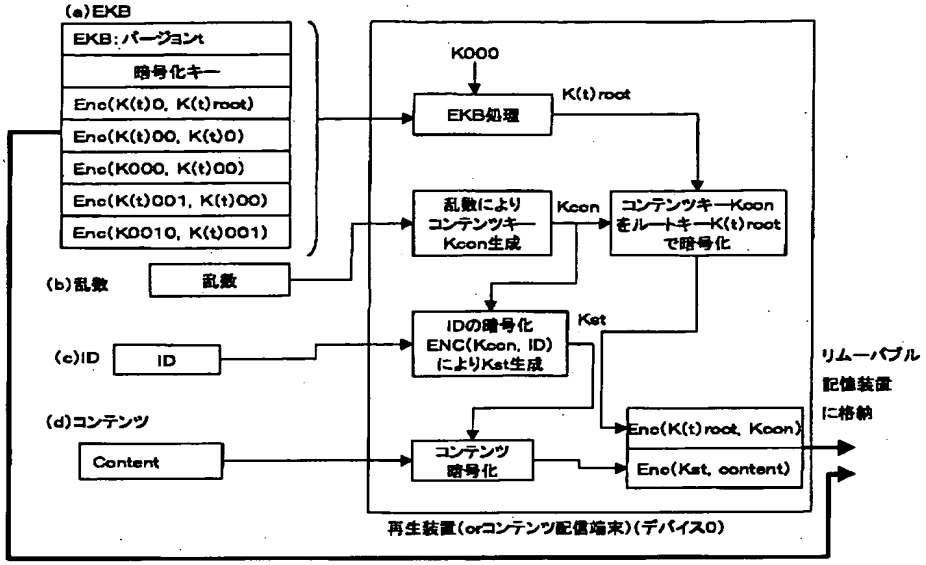
簡略化した有効化キーブロック(EKB:Enabling Key Block)を用いた
デバイスKa, Kg, Kjへのバージョンｔのコンテンツキー送付処理



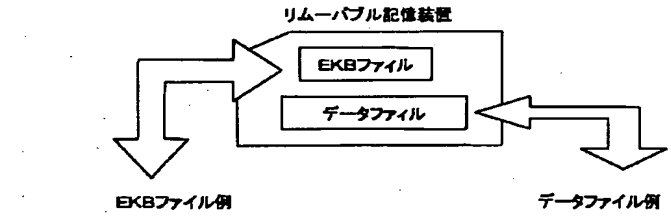
【図１５】



【図１６】



【図１７】



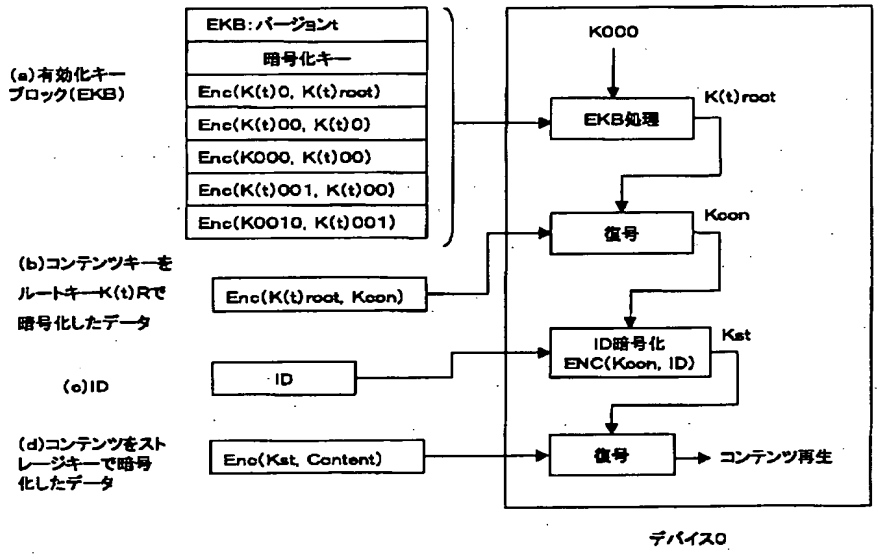
EKBファイル例

バージョン(Version):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)root)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

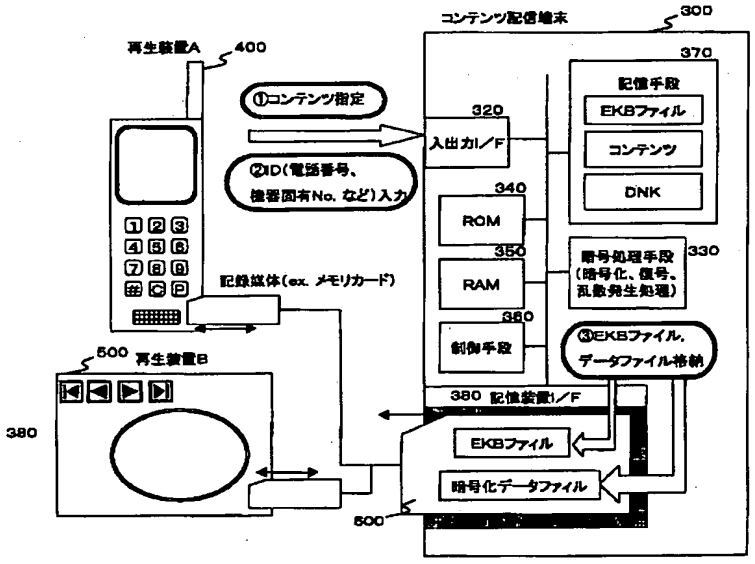
データファイル例

対応EKBバージョン(Version):t
Enc(Kroot, Kcon)
Enc(Kst, CONTENT(DATA))

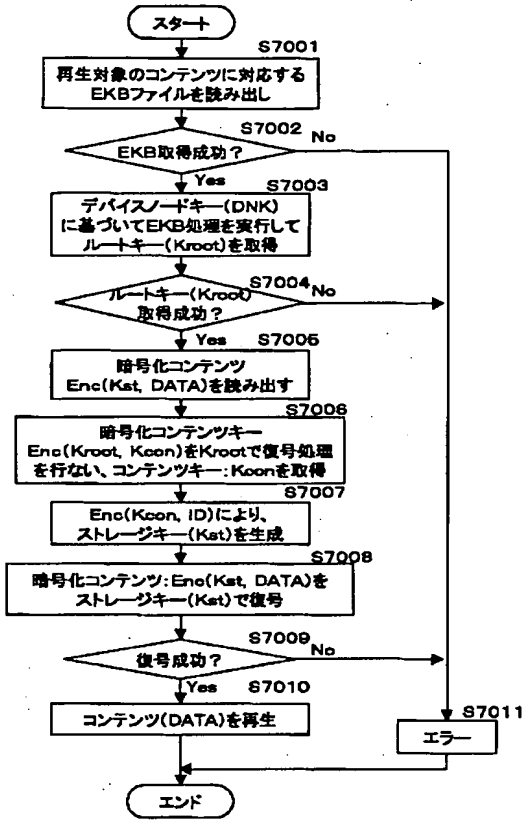
【図１８】


EKB:バージョンt
暗号化キー
Enc(K(t)0, K(t)root)
Enc(K(t)00, K(t)0)
Enc(K000, K(t)00)
Enc(K(t)001, K(t)00)
Enc(K0010, K(t)001)
(a)有効化キーブロック(EKB)
K000
EKB処理
K(t)root
復号
Koon
(b)コンテンツキーをルートキーK(t)Rで暗号化したデータ
Enc(K(t)root, Koon)
ID暗号化 ENC(Koon, ID)
Kst
(c)ID
ID
(d)コンテンツをストレージキーで暗号化したデータ
Enc(Kst, Content)
復号
コンテンツ再生
デバイス0

【図１９】


コンテンツ配信端末
300
再生装置A
400
①コンテンツ指定
②ID(電話番号、機器固有No. など)入力
記録媒体(ex. メモリカード)
320
入出力I/F
340
ROM
350
RAM
360
制御手段
370
記憶手段
EKBファイル
コンテンツ
DNK
暗号処理手段(暗号化、復号、乱数発生処理)
330
③EKBファイル、データファイル格納
380 記憶装置I/F
EKBファイル
暗号化データファイル
500
500 再生装置B
380

【図２２】


スタート
S7001
再生対象のコンテンツに対応する
EKBファイルを読み出し
S7002
EKB取得成功？
No
Yes
S7003
デバイスノードキー(DNK)
に基づいてEKB処理を実行して
ルートキー(Kroot)を取得
S7004
ルートキー(Kroot)
取得成功？
No
Yes
S7005
暗号化コンテンツ
Enc(Kst, DATA)を読み出す
S7006
暗号化コンテンツキー
Enc(Kroot, Kcon)をKrootで復号処理
を行ない、コンテンツキー:Kconを取得
S7007
Enc(Kcon, ID)により、
ストレージキー(Kst)を生成
S7008
暗号化コンテンツ:Enc(Kst, DATA)を
ストレージキー(Kst)で復号
S7009
復号成功？
No
Yes
S7010
コンテンツ(DATA)を再生
S7011
エラー
エンド